Privacy Button IP7133/IP7134

NETWORK CAMERA

User's Manual

VIVOTEK
www.vivotek.com

IP Surveillance

Table of Contents

Overview

VIVOTEK IP7133 (Wired)/IP7134 (Wireless) is an easy-to-use network camera, specifically designed for home security applications with a compact, stylish exterior. Despite its ultra-compact size, it incorporates with a good many advanced features to fit your needs.

Embedded with the VIVOTEK VVTK-1000 SoC, it enables to simultaneously deliver dual streams in MPEG-4 and MJPEG with different video resolution and quality upon different devices such as PC or 3G cell phones. With this network camera, you can quickly, easily access it to view the current status of your children, the elderly, or even your pets with live, clear videos while you're away from home. IP7134 also supports built-in 802.11b/g WLAN capability, which can prevent your elegant home decoration from tangled cablings.

Additionally, it comes with a push button on the front side for privacy use. You are able to manually stop the operation of video monitoring with ease while getting back home. This considerate design avoids the feeling of being monitored all day long. With the delicate design and versatile functions, VIVOTEK IP7133/IP7134 is definitely the best choice for the fundamental establishment of home security.

Read before use

The use of surveillance devices may be prohibited by law in your country. The Network Camera is not only a high-performance web-ready camera but also can be part of a flexible surveillance system. It is the user's responsibility to ensure that the operation of such devices is legal before installing this unit for its intended use.

It is important to first verify that all contents received are complete according to the Package contents listed below. Take notice of the warnings in Quick Installation Guide before the Network Camera is installed; then carefully read and follow the instructions in the Installation chapter to avoid damages due to faulty assembly and installation. This also ensures the product is used properly as intended.

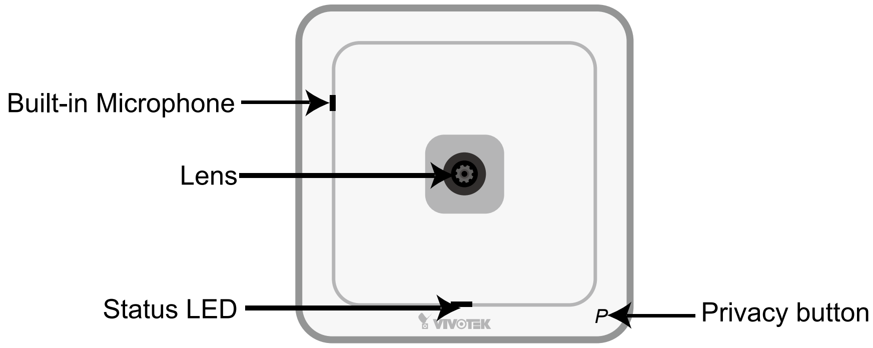
The Network Camera is a network device and its use should be straightforward for those who have basic network knowledge. It is designed for various applications including video sharing, general security/surveillance, etc. The Configuration chapter suggests ways to best utilize the Network Camera and ensure proper operations. For the creative and professional developers, the URL Commands of the Network Camera section serves to be a helpful reference to customize existing homepages or integrating with the current web server.

Package contents

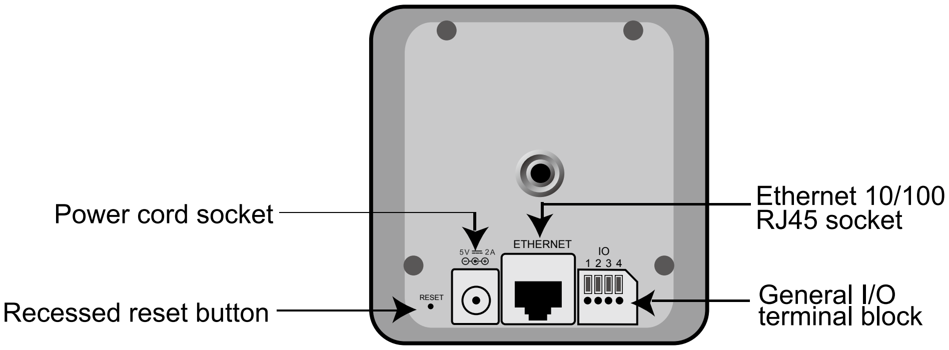
- IP7133/IP7134
- Power adapter
- Camera stand
- Software CD
- Warranty card
- Quick installation guide
- Screws

Physical description

Front panel

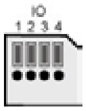


Connectors



General I/O Terminal Block

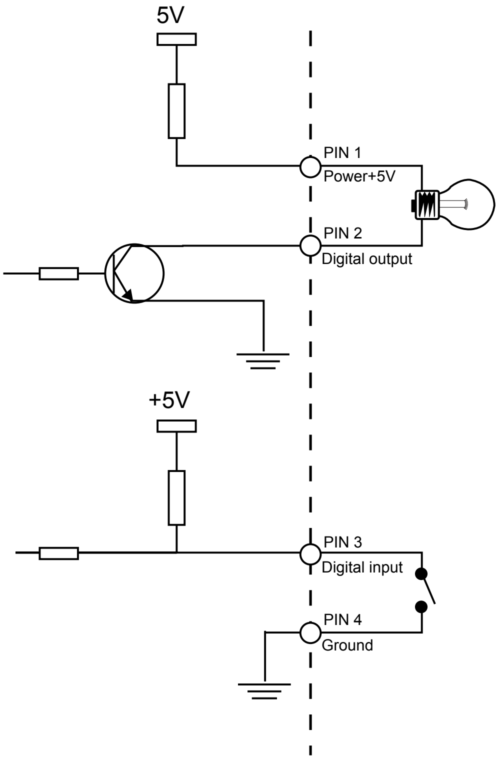
This Network Camera provides a general I/O terminal block which is used to connect external input / output devices. The pin definitions are described below.



1: Power
2: Digital output
3: Digital input
4: Ground

DI/DO Diagram

Refer to the following illustration for connection method.

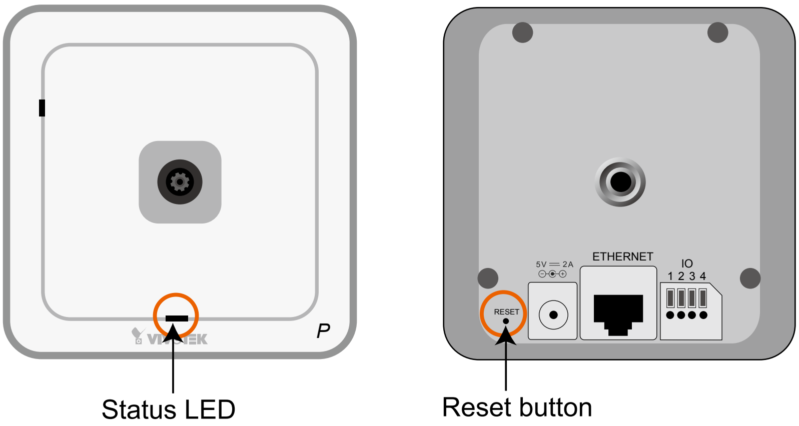


Status LED

The LED indicates the status of the Network Camera.

Status LED	Privacy button	Description
Solid red	Solid blue	Power is being supplied to the camera.
Blinking red	Blinking blue	The camera is booting up.
Solid red	OFF	The camera is trying to obtain an IP address.
Blinking green	OFF	An IP address has been successfully assigned to the camera and the camera is working.
Blinking red	OFF	During firmware upgrading.
Blinking green and red	OFF	Restore the camera.

Hardware Reset



There is a reset button on the back cover of the Network Camera. It is used to reboot the Network Camera or restore the Network Camera to factory default. Sometimes rebooting the Network Camera could set the Network Camera back to normal state. If the problems remain after rebooted, restore the Network Camera to factory default and install again.

Reboot: Press and release the reset button. The status LED will blinks in red.

Restore: Press the reset button continuously until the status LED blinks in red and green simultaneously. Note that all settings will be restored to factory default.

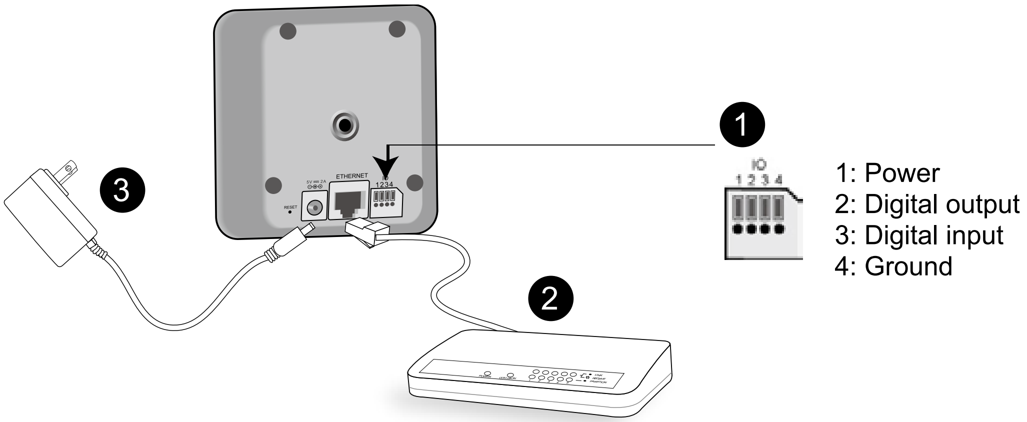
Installation

Network deployment

Setup the Network Camera over the Internet

This section explains how to configure the Network Camera to Internet connection.

1. If you have external devices such as sensors and alarms, make connection from general I/O terminal block.
2. Connect the camera to a switch via Ethernet cable. Use Catagory 5 Cross Cable when Network Camera is directly connected to PC.
3. Connect the supplied power cable from the Network Camera to a power outlet.

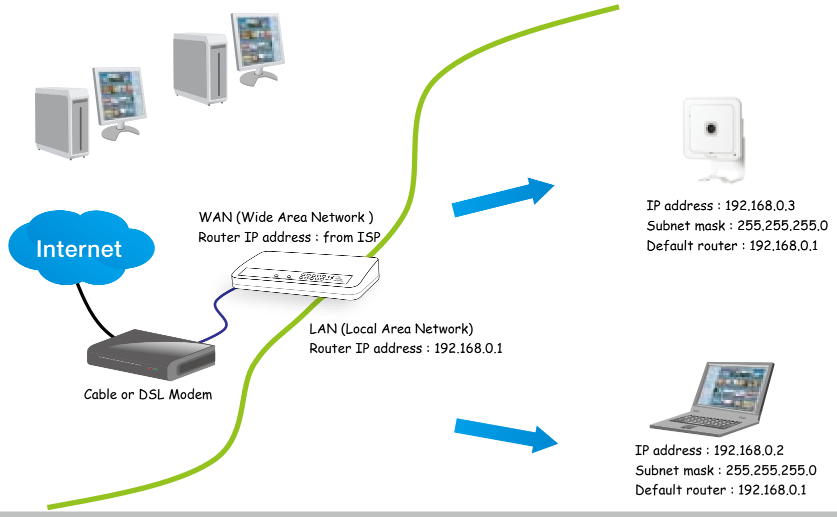


There are several ways to setup the Network Camera over the Internet. The first way is to setup the Network Camera behind a router. The second way is to utilize a static IP. The third way is to use PPPoE.

Internet connection via a router

Before setting up the Network Camera over the Internet, make sure you have a router and follow the steps below.

1. Connect your Network Camera behind a router, the Internet environment is illustrated as below. About how to get your IP address, please refer to Software installation on page 9 for details.


Internet
WAN (Wide Area Network)
Router IP address : from ISP
LAN (Local Area Network)
Router IP address : 192.168.0.1
Cable or DSL Modem
IP address : 192.168.0.3
Subnet mask : 255.255.255.0
Default router : 192.168.0.1
IP address : 192.168.0.2
Subnet mask : 255.255.255.0
Default router : 192.168.0.1

2. In this case, if the Local Area Network (LAN) IP address of your Network Camera is 192.168.0.3, please forward the following ports for the Network Camera on the router.

■ HTTP port
■ RTSP port
■ RTP port for audio
■ RTCP port for audio
■ RTP port for video
■ RTCP port for video

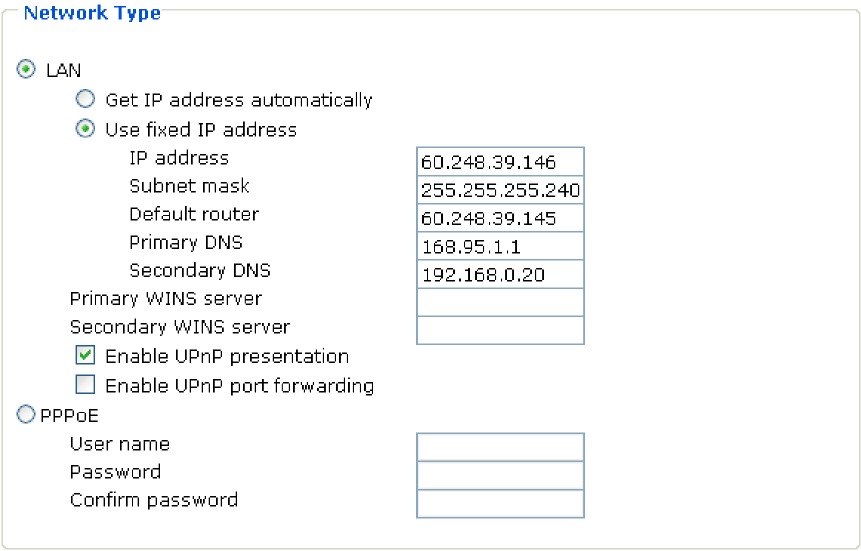
If you have changed the port numbers on the Network page, please open the ports accordingly on your router. For information on how to forward ports on the router, please refer to the user's manual of your router.

3. Find out the public IP address of your router provided by your ISP (Internet Service Provider). Use the public IP and the secondary HTTP port to access the Network Camera from the Internet. Please refer to Network Type on page 23 for details.

Internet connection with static IP

Choose this connection type if you are required to use a static IP for the Network Camera and follow the steps below.

1. Set up the Network Camera in LAN. Please refer to Software installation on page 9 for details.
2. Go to Configuration > Network > Network Type. Select LAN > Use fixed IP address.
3. Enter the static IP, Subnet mask, Default router, Primary DNS provided by your ISP.



Network Type

● LAN

○ Get IP address automatically

● Use fixed IP address

IP address	60.248.39.146
Subnet mask	255.255.255.240
Default router	60.248.39.145
Primary DNS	168.95.1.1
Secondary DNS	192.168.0.20
Primary WINS server	
Secondary WINS server	

☑ Enable UPnP presentation

□ Enable UPnP port forwarding

○ PPPoE

User name	
Password	
Confirm password	

Internet connection via PPPoE (Point-to-Point over Ethernet)

Choose this connection type if you are connected to the Internet via a DSL Line. Please refer to PPPoE on page 24 for details.

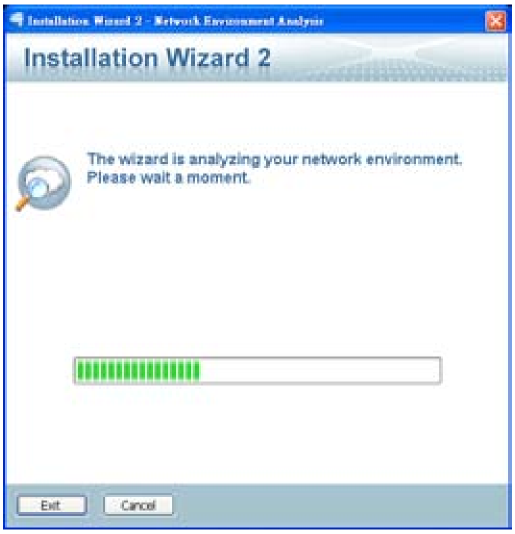
Software installation

Installation Wizard 2 (IW2), free-bundled software packaged in the product CD, helps to set up your Network Camera in LAN.

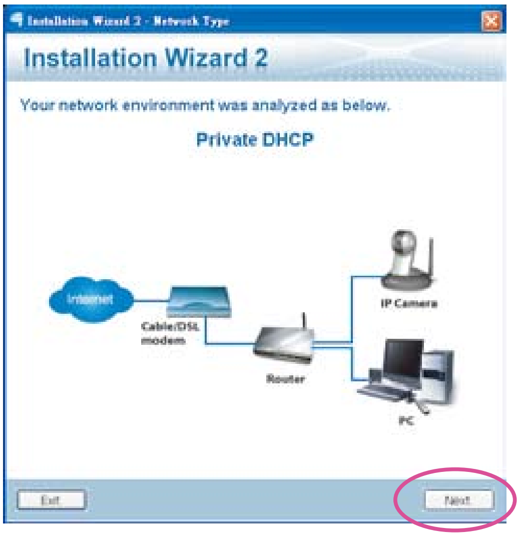
1. Install the IW2 under the Software Utility directory from the software CD. Double click the IW2 shortcut on your desktop to launch the program.

Installation Wizard 2

2. The program will conduct analyses on your network environment. After your network environment is analyzed, please click Next to continue the program.



The wizard is analyzing your network environment. Please wait a moment.

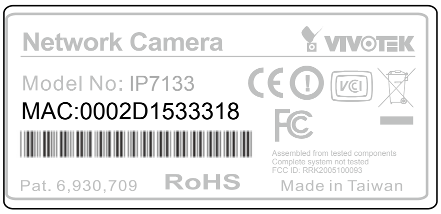


Your network environment was analyzed as below.

Private DHCP

3. The program will search all VIVOTEK devices on the same LAN.

4. After searching, the main installer window will pop up. Click on the MAC and model name which match the product label on your device to connect to the Network Camera.



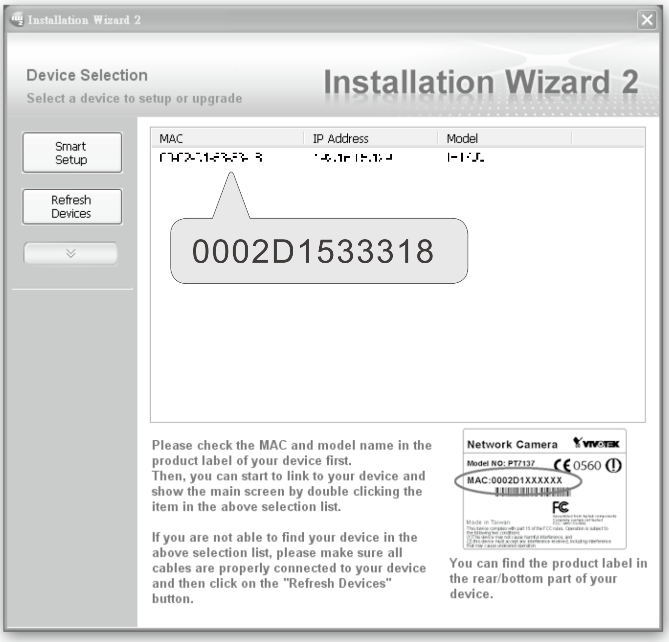
Network Camera VIVOTEK

Model No: IP7133

MAC:0002D1533318

Assembled from tested components
Complete system not tested
FCC ID: RRK2005100093

Pat. 6,930,709 RoHS Made in Taiwan



Please check the MAC and model name in the product label of your device first.
Then, you can start to link to your device and show the main screen by double clicking the item in the above selection list.

If you are not able to find your device in the above selection list, please make sure all cables are properly connected to your device and then click on the "Refresh Devices" button.

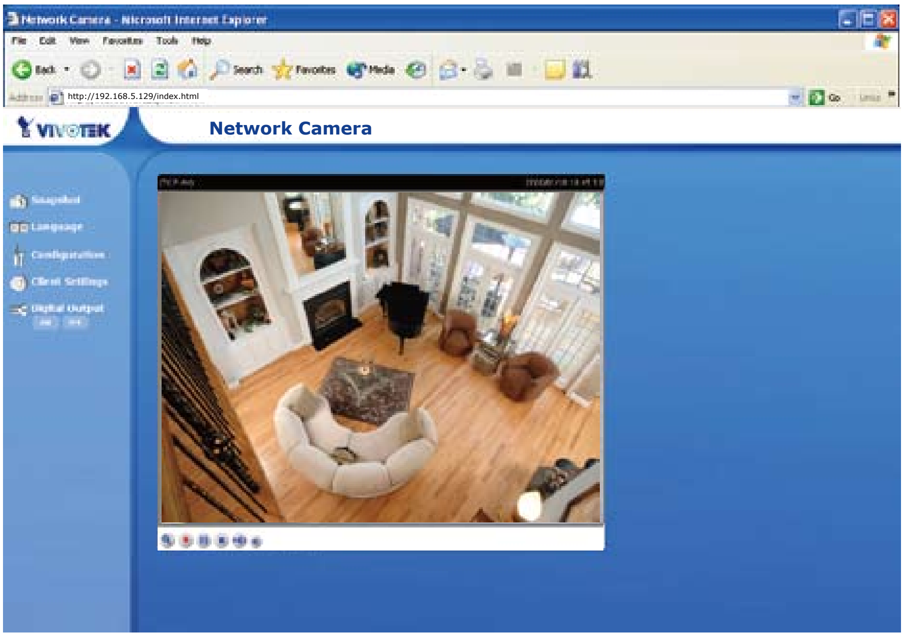
You can find the product label in the rear/bottom part of your device.

Accessing the Network Camera

This chapter explains how to access the Network Camera through web browsers, RTSP players, 3GPP-compatible mobile devices, and VIVOTEK recording software.

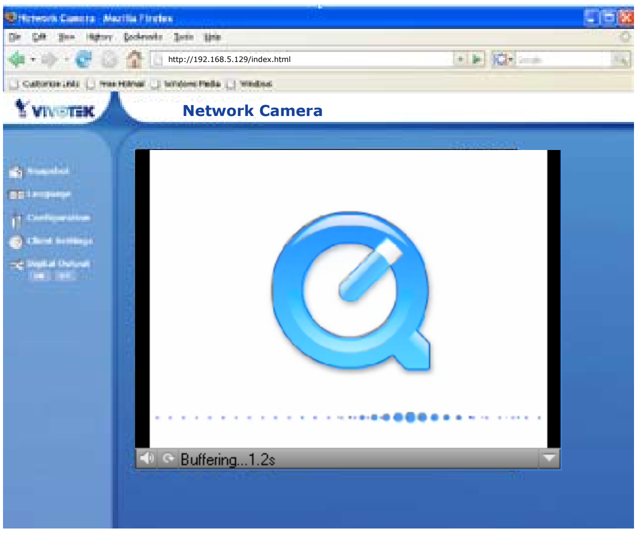
Using web browsers

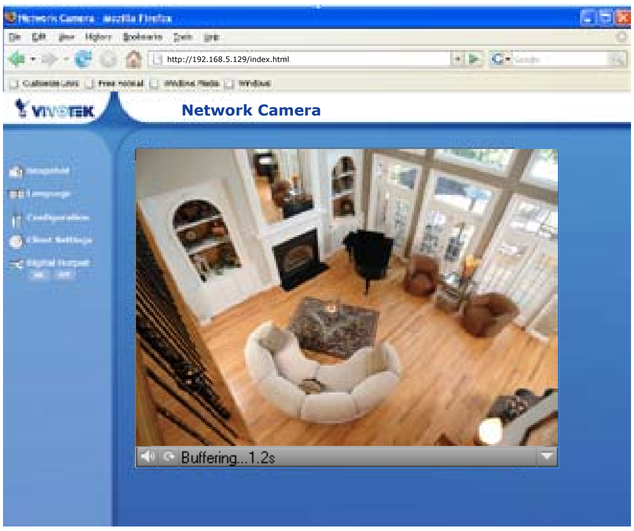
1. Launch your web browser (ex. Microsoft® Internet Explorer, Mozilla Firefox or Netscape).
2. Enter the IP address of the Network Camera in the address field. Press **Enter**.
3. The live video will be displayed in your web browser.


Network Camera - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.5.129/index.html Go Links
VIVOTEK
Network Camera
Snapshot
Language
Configuration
Client Settings
Digital Output

NOTE

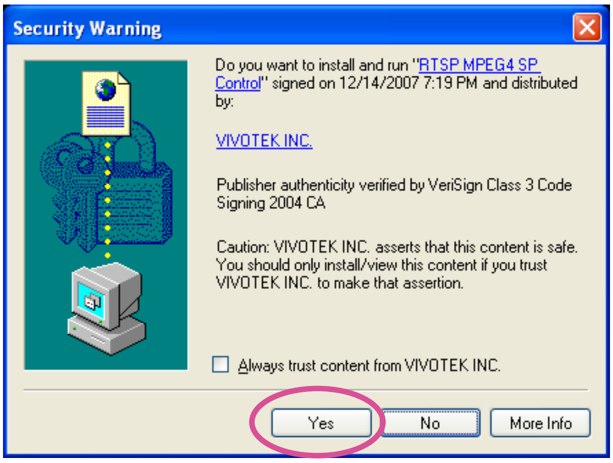
► *For Mozilla Firefox or Netscape users, your browser will use Quick Time to stream the live video.*


Network Camera - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.5.129/index.html
VIVOTEK
Network Camera
Snapshot
Language
Configuration
Client Settings
Digital Output
Buffering...1.2s


Network Camera - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.5.129/index.html
VIVOTEK
Network Camera
Snapshot
Language
Configuration
Client Settings
Digital Output
Buffering...1.2s

- *By default, the Network Camera is not password-protected. To prevent unauthorized accesses, it is highly recommended to set a password for the Network Camera.*
  For more information about how to enable password protection, please refer to Security on page 22.

- *If you see a warning message at initial access, click Yes to install an ActiveX® control on your computer.*



Security Warning

Do you want to install and run "RTSP MPEG4 SP Control" signed on 12/14/2007 7:19 PM and distributed by:

VIVOTEK INC.

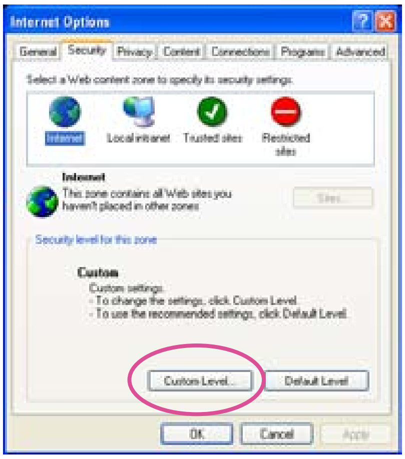
Publisher authenticity verified by VeriSign Class 3 Code Signing 2004 CA

Caution: VIVOTEK INC. asserts that this content is safe. You should only install/view this content if you trust VIVOTEK INC. to make that assertion.

□ Always trust content from VIVOTEK INC.

- *If you see a dialog box indicating that your security settings prohibit running ActiveX® Controls, please enable your ActiveX® Controls for your browser.*

1. Choose Tools > Internet Options > Security > Custom Level.



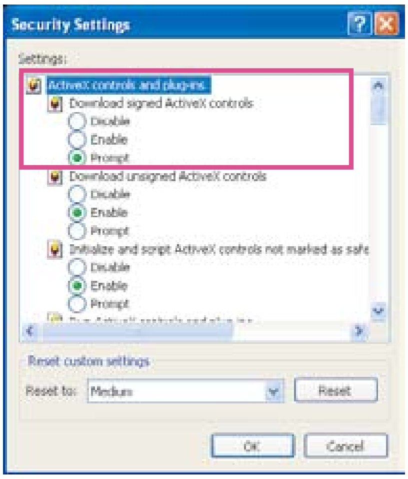
Select a Web content zone to specify its security settings.

Internet
This zone contains all Web sites you haven't placed in other zones

Security level for this zone

Custom
Custom settings.
- To change the settings, click Custom Level.
- To use the recommended settings, click Default Level.

2. Look for Download signed ActiveX® controls; select Enable or Prompt. Click ***OK****.*



Settings:

ActiveX controls and plug-ins
Download signed ActiveX controls
○ Disable
○ Enable
● Prompt
Download unsigned ActiveX controls
○ Disable
● Enable
○ Prompt
Initialize and script ActiveX controls not marked as safe
○ Disable
● Enable
○ Prompt

Reset custom settings
Reset to: Medium

Using RTSP players

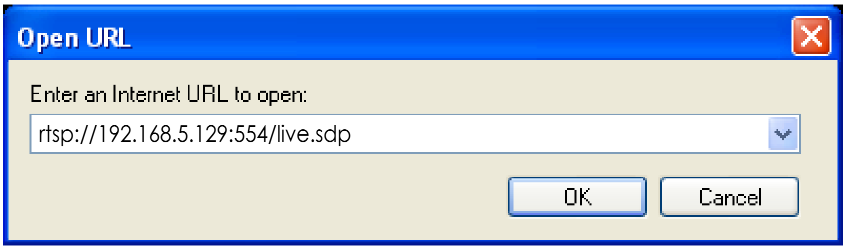
To view the MPEG-4 streaming media using RTSP players, you can use one of the following players that support RTSP streaming.

Quick Time Player

Real Player

1. Launch a RTSP player.
2. Choose File > Open URL. An URL dialog box will pop up.
3. Type the URL command in the text box.
   The format is rtsp://<ip address>:<rtsp port>/<RTSP Streaming access name for stream1 or stream2>

   For example:

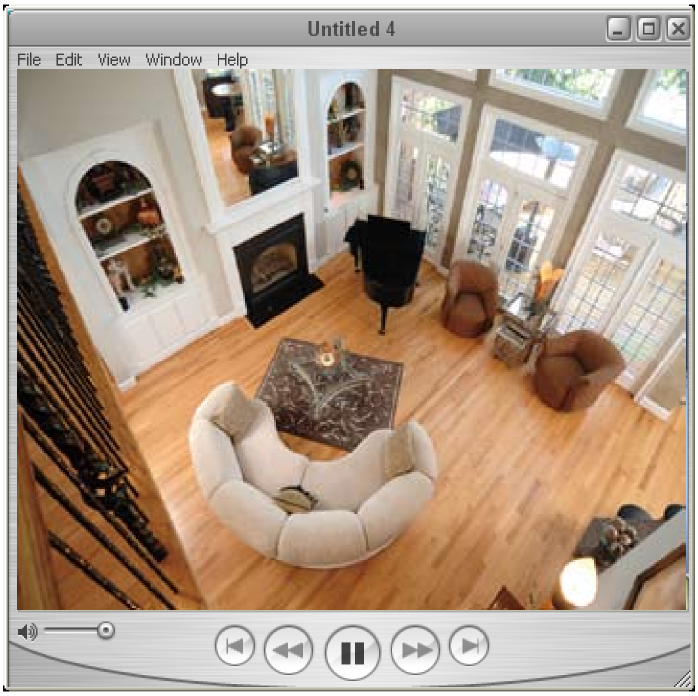


Open URL

Enter an Internet URL to open:

rtsp://192.168.5.129:554/live.sdp

4. The live video will be displayed in your player.
   For more information on how to configure RTSP access name, please refer to RTSP Streaming on page 28 for details.



Using 3GPP-compatible mobile devices

To view the streaming media through 3GPP-compatible mobile devices, make sure the Network Camera can be accessed from the Internet. For more information on how to set up the Network Camera over the Internet, please refer to Setup the Network Camera over the Internet on page 7.

To utilize this feature, please check the following settings on your Network Camera:

1. Because most players on 3GPP mobile phones do not support RTSP authentication, make sure the authentication mode of RTSP streaming is set to disable.
   For more information, please refer to RTSP Streaming on page 28.

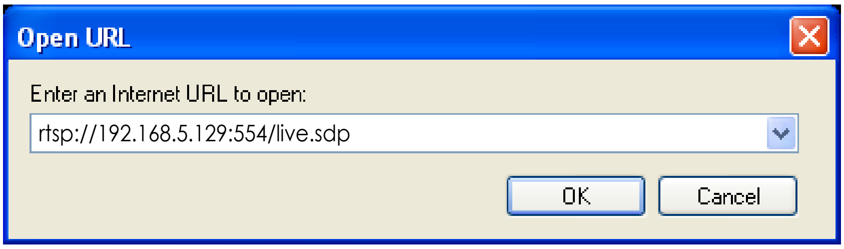
2. As the 3G network bandwidth is limited, you can’t use large video size. Please set the video and audio streaming parameters as listed below.
   For more information, please refer to Audio and video on page 36.

Video Mode	MPEG-4
Frame size	176 x 144
Maximum frame rate	5 fps
Intra frame period	1S
Video quality (Constant bit rate)	40kbps
Audio type (GSM-AMR)	12.2kbps

3. As most ISP and players only support port number 554 to allow RTSP streaming to go through, please set the RTSP port to 554.For more information, please refer to RTSP Streaming on page 28.

4. Launch the players on 3GPP-compatible mobile devices, (ex. Real Player).
   Type the URL commands in the player.
   The format is rtsp://<public ip address of your camera>:<rtsp port>/<RTSP Streaming access name for stream1 or stream2>.

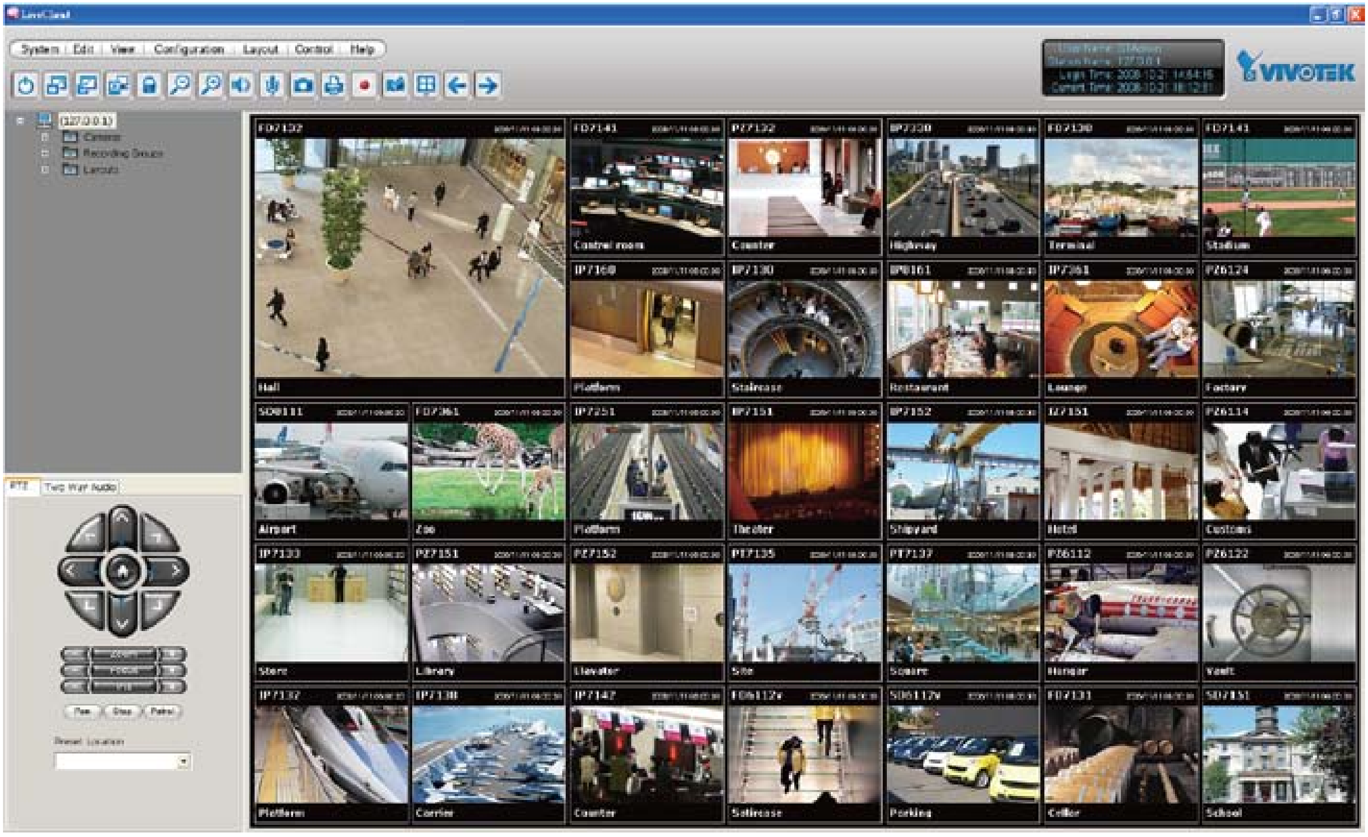
   For example:



Enter an Internet URL to open:
rtsp://192.168.5.129:554/live.sdp

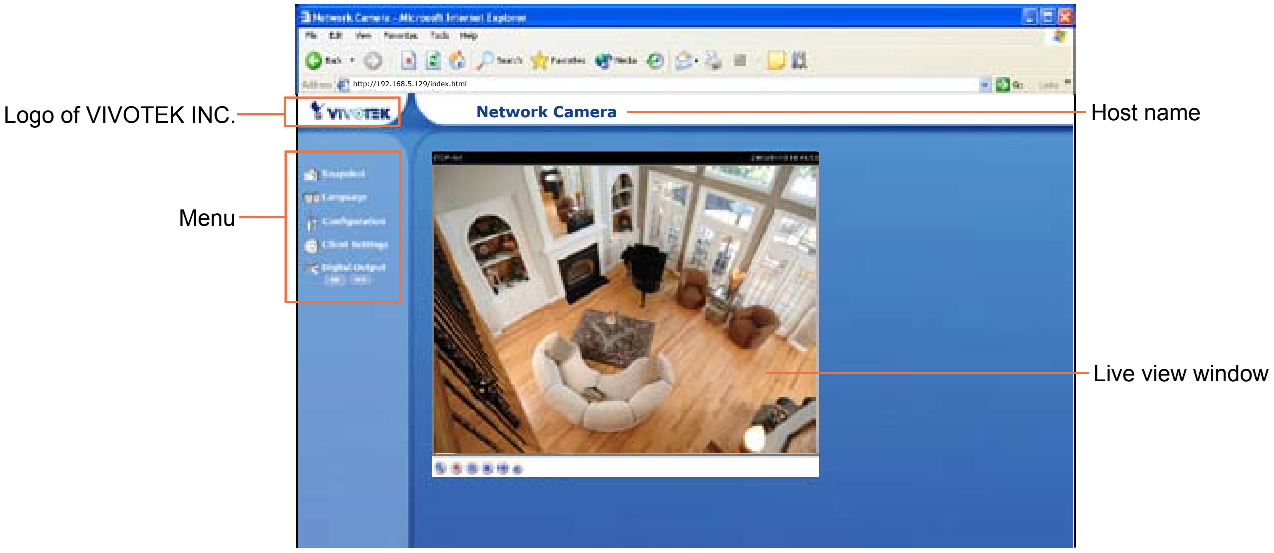
Using VIVOTEK recording software

The product software CD also contains VIVOTEK's recording software, allowing simultaneous monitoring and video recording for multiple Network Cameras. Please install the recording software, then launch the program to add the Network Camera to the Channel list. For detailed information about how to use the recording software, please refer to the user's manual of the software or download the manual from http://www.vivotek.com.



Main Page

This chapter explains the layout of the main page. It is composed of the following four sections: VIVOTEK INC. Logo, Menu, Host Name, and Live Video Window.



VIVOTEK INC. Logo

Click this logo to visit VIVOTEK website.

Menu

Snapshot: Click this button to capture and save still images. The captured images will be displayed in a pop-up window. Right-click the image and choose Save Picture As to save it in JPEG (*.jpg) or BMP (*.bmp) format.

Language: Click this button to choose a language for the displayed interface. Language options are available in: English, Deutsch, Español, Français, Italiano, 日本語, Português, 簡体中文, and 繁體中文.

Configuration: Click this button to access the configuration page of Network Camera. It is suggested that a password is applied to the Network Camera so that only the administrator can configure the Network Camera. For more information, please refer to Configuration on page 20.

Client Settings: Click this button to access the client setting page. For more information, please refer to Client Settings on page 18.

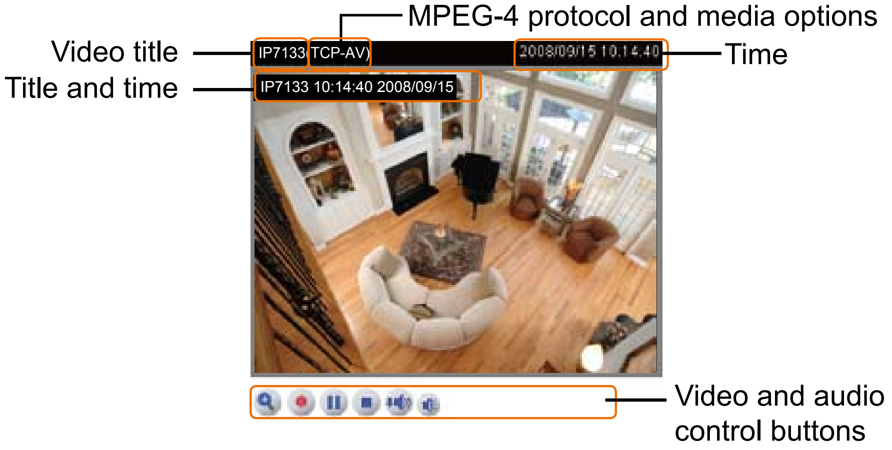
Digital Output: Click this button to turn on or off the digital output device.

Host Name

The host name can be customized to fit your needs. For more information, please refer to System on page 20.

Live Video Window

The following window is displayed when the video mode is set to MPEG-4:


MPEG-4 protocol and media options
Video title
IP7133
TCP-AV
2008/09/15 10:14:40
Time
Title and time
IP7133 10:14:40 2008/09/15
Video and audio control buttons

Video title: The video title can be configured. For more information, please refer to Video settings on page 36.

Time: Display the current time. For more information, please refer to Video settings on page 36.

Title and time: Video title and time can be stamped on the streaming video. For more information, please refer to Video settings on page 36.

MPEG-4 protocol and media options: The transmission protocol and media options for MPEG-4 video streaming. For more information, please refer to Client Settings on page 18.

Video and audio control buttons: Depending on the Network Camera model and Network Camera configuration, some buttons may not be available.

🔍 Digital zoom edit: Uncheck Disable digital zoom to enable the zoom operation. The navigation screen indicates which part of the image is being magnified. To control the zoom level, drag the slider bar. To move to a different area you want to magnify, drag the navigation screen.

● Start MP4 recording: Click this button to record video clips in MP4 file format to your computer. Press the ● Stop MP4 recording button to end recording. When you exit the web browser, video recording stops accordingly. To specify the storage destination and the file name, please refer to MP4 Saving Options on page 19 for details.

⏸ Pause: Pause the transmission of streaming media. The button becomes ▶ Resume button after clicking the Pause button.

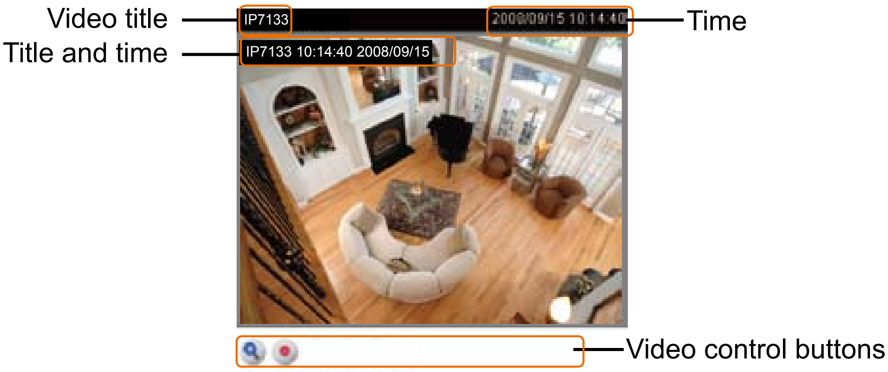
▶ Resume: Resume the transmission of streaming media. The button becomes ⏸ Pause button after clicking the Resume button.

■ Stop: Stop the transmission of streaming media. Click the ▶ Resume button to continue transmission.

🔊 Volume: When the 🔇 mute function is not activated, move the slider bar to adjust the volume at local computer.

🔇 Mute: Turn off the 🔊 volume at local computer. Click 🔇 to turn on the audio function.

The following window is displayed when the video mode is set to MJPEG:



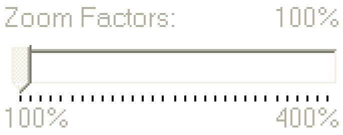
Video title: The video title can be configured. For more information, please refer to Video settings on page 36.

Time: Display the current time. For more information, please refer to Video settings on page 36.

Title and time: Video title and time can be stamped on the streaming video. For more information, please refer to Video settings on page 36.

Video control buttons: Depending on the Network Camera model and Network Camera configuration, some buttons may not be available.

🔍 Digital zoom edit: Uncheck Disable digital zoom to enable the zoom operation. The navigation screen indicates which part of the image is being magnified. To control the zoom level, drag the slider bar. To move to a different area you want to magnify, drag the navigation screen.

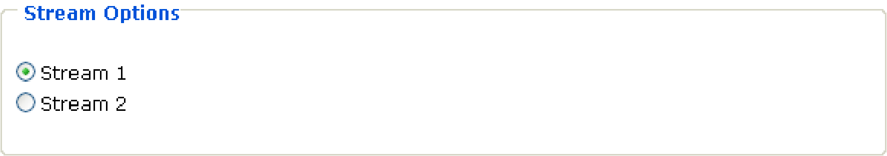


● Start MP4 recording: Click this button to record video clips in MP4 file format to your computer. Press the ● Stop MP4 recording button to end recording. When you exit the web browser, video recording stops accordingly. To specify the storage destination and the file name, please refer to MP4 Saving Options on page 19 for details.

Client Settings

This chapter explains how to select the streaming source, transmission mode and saving options at local computer. It is composed of the following four sections: Stream Options, MPEG-4 Media Options, MPEG-4 Protocol Options and MP4 Saving Options. When completed with the settings on this page, click **Save** on the page bottom to enable the settings.

Stream Options

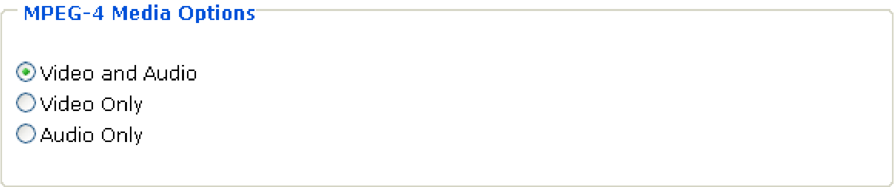


Stream Options

● Stream 1
○ Stream 2

The Network Camera supports MPEG-4 and MJPEG dual streams. For more information, please refer to Video settings on page 36.

MPEG-4 Media Options

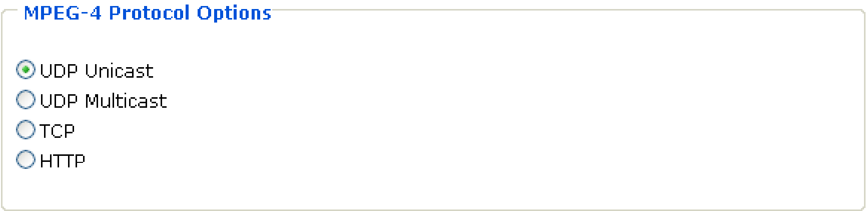


MPEG-4 Media Options

● Video and Audio
○ Video Only
○ Audio Only

Select to stream video or audio data. This works only when the video mode is set to MPEG-4.

MPEG-4 Protocol Options



MPEG-4 Protocol Options

● UDP Unicast
○ UDP Multicast
○ TCP
○ HTTP

Depending on your network environment, there are four transmission modes of MPEG-4 streaming:

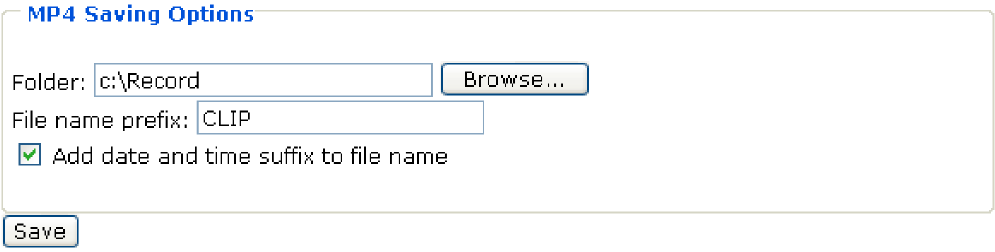
UDP unicast: This protocol allows for more real-time audio and video streams. However, network packets may be lost due to network burst traffic and images may be broken. Activate UDP connection when occasions require time-sensitive responses and the video quality is less important. Note that each unicast client connecting to the server takes up additional bandwidth and the Network Camera allows up to ten simultaneous accesses.

UDP multicast: This protocol allows multicast-enabled routers to forward network packets to all clients requesting streaming media. This helps to reduce the network transmission load of the Network Camera while serving multiple clients at the same time. Note that to utilize this feature, the Network Camera must be configured to enable multicast streaming at the same time. For more information, see RTSP Streaming on page 34.

TCP: This protocol guarantees the complete delivery of streaming data and thus provides better video quality. Nevertheless, the downside with this protocol is that its real-time effect is not as good as that of the UDP protocol.

HTTP: This protocol allows the same quality as TCP protocol and you don't need to open specific port for streaming under some network environments. Users inside a firewall can utilize this protocol to allow streaming data to come through.

MP4 Saving Options



MP4 Saving Options

Folder: c:\Record

File name prefix: CLIP

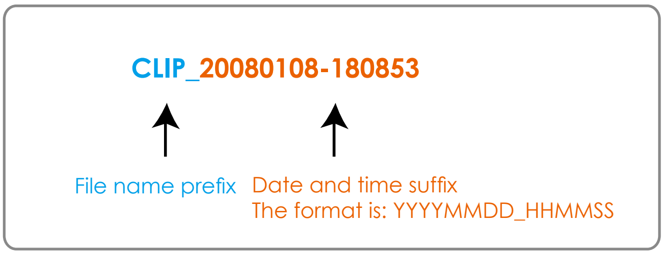
☑ Add date and time suffix to file name

Users can record the live video as they are watching it by clicking ● Start MP4 Recording on the main page. Here, you can specify the storage destination and file name.

Folder: Specify a storage destination for the recorded video files.

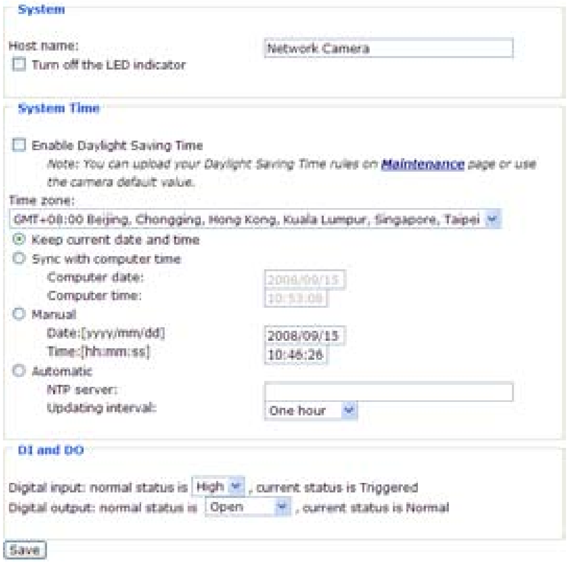
File Name Prefix: Enter the text that will be put in front of the video file name.

Add date and time suffix to the file name: Select this option to add date and time to the file name suffix.



Configuration

Only Administrators can access the system configuration page. Each category in the left menu will be explained in the following sections.



System

Host name: Network Camera

□ Turn off the LED indicator

System Time

□ Enable Daylight Saving Time

Note: You can upload your Daylight Saving Time rules on **Maintenance** *page or use the camera default value.*

Time zone:

GMT+08:00 Beijing, Chongqing, Hong Kong, Kuala Lumpur, Singapore, Taipei

● Keep current date and time

○ Sync with computer time

Computer date: 2008/09/15

Computer time: 10:53:08

○ Manual

Date:[yyyy/mm/dd] 2008/09/15

Time:[hh:mm:ss] 10:46:26

○ Automatic

NTP server:

Updating interval: One hour

DI and DO

Digital input: normal status is High , current status is Triggered

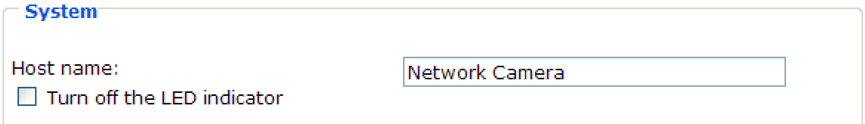
Digital output: normal status is Open , current status is Normal

Save

System

This section explains how to configure the basic settings for the Network Camera, such as the host name and system time. It is composed of the following three columns: System, System Time and DI and DO. When completed with the settings on this page, click Save on the page bottom to enable the settings.

System



System

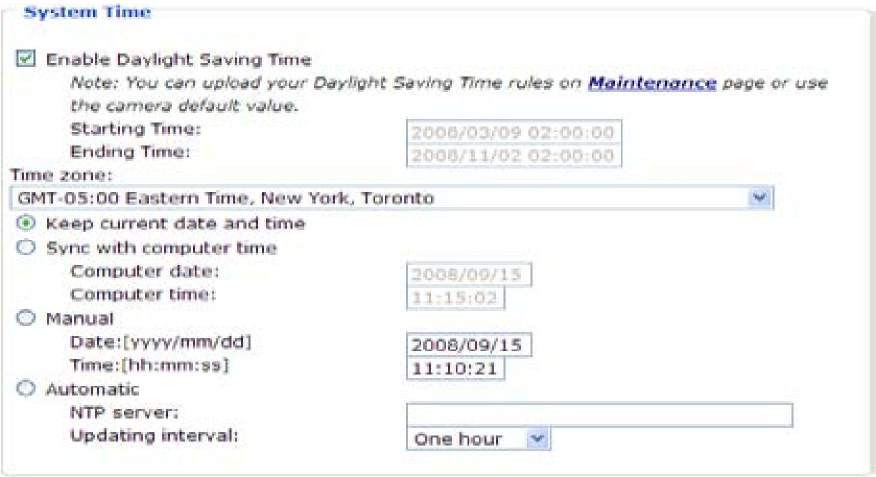
Host name: Network Camera

□ Turn off the LED indicator

Host name: Set a desired name for the Network Camera. The text will be displayed at the top of the main page.

Turn of the LED indicators: If you don't want to let others know that the network camera is on, you can select this option to turn off the LED indicators.

System Time



System Time

☑ Enable Daylight Saving Time

Note: You can upload your Daylight Saving Time rules on **Maintenance** *page or use the camera default value.*

Starting Time: 2008/03/09 02:00:00

Ending Time: 2008/11/02 02:00:00

Time zone:

GMT-05:00 Eastern Time, New York, Toronto

● Keep current date and time

○ Sync with computer time

Computer date: 2008/09/15

Computer time: 11:15:02

○ Manual

Date:[yyyy/mm/dd] 2008/09/15

Time:[hh:mm:ss] 11:10:21

○ Automatic

NTP server:

Updating interval: One hour

Time zone: According to your local time zone, select one from the drop-down list.

Keep current date and time: Select this option to reserve the current date and time of the Network Camera. The Network Camera's internal real-time clock maintains the date and time even when the power of the system is turned off.

Sync with computer time: Select this option to synchronize the date and time of the Network Camera with the local computer. The read-only date and time of the PC is displayed as updated.

Manual: The administrator can enter the date and time manually. Note that the date and time format are [yyyy/mm/dd] and [hh:mm:ss].

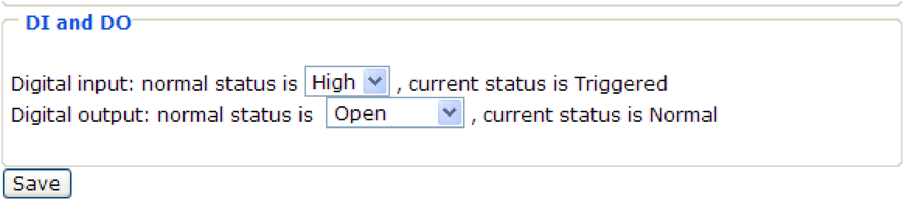
Automatic: The Network Time Protocol is a protocol serves synchronize computer clocks by periodically querying an NTP Server.

NTP server: Assign the IP address or domain name of the time-server. Leaving the text box blank connects the Network Camera to the default time-servers.

Update interval: Select to update the time with the NTP server on hourly, daily, weekly, or monthly basis.

Enable Daylight Saving Time: Select this option to enable daylight saving time (DST). During DST, the system clock moves one hour ahead.
Please follow the steps below to enable daylight saving time:
1. Select the time zone for your Network Camera first.
2. Select Enable Daylight Saving Time.
3. The starting time and ending time of the DST will be displayed in this option.
4. To manually configure the daylight saving time rules, please refer to Upload / Export Daylight Saving Time Configuration File on page 53 for details.

DI and DO



DI and DO

Digital input: normal status is High, current status is Triggered

Digital output: normal status is Open, current status is Normal

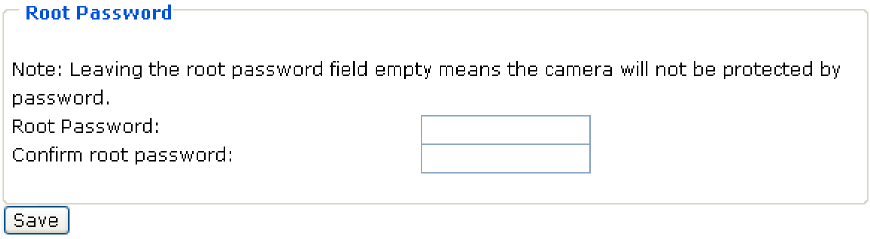
Digital input: Select High or Low to define normal status of the digital input. The Network Camera will report the current status.

Digital output: Select Grounded or Open to define normal status of the digital output. The Network Camera will show whether the trigger is activated or not.

Security

This section explains how to enable password protection and create multiple accounts. It is composed of the following three columns: Root Password, Add User and Manage User.

Root Password



Root Password

Note: Leaving the root password field empty means the camera will not be protected by password.

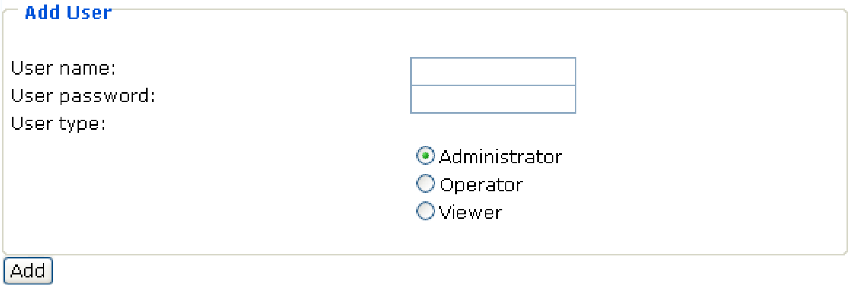
Root Password:

Confirm root password:

The administrator account “root” is permanent and can not be deleted. Please note that if you want to add more accounts, you must apply a password for the “root” account first.

1. Type the password identically in both text boxes.
2. Click Save to enable password protection.
3. A window will be prompted for authentication; type the correct user’s name and password in related fields to access the Network Camera.

Add User



Add User

User name:

User password:

User type:

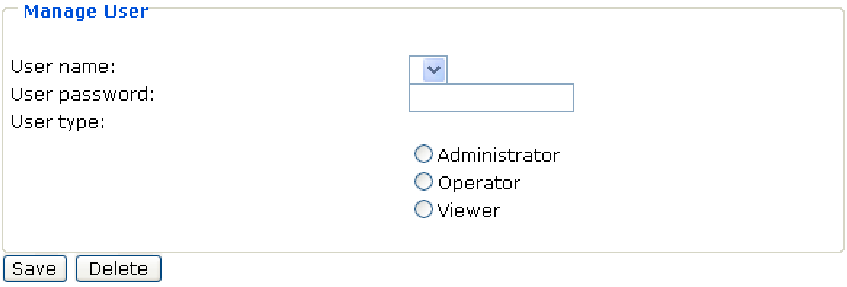
● Administrator
○ Operator
○ Viewer

Administrators can add up to twenty user accounts.

1. Input the new user’s name and password.
2. Select the desired security level. Click **Add** to enable the settings.

Access rights are sorted by user types. There are three kinds of user types. Only administrators can access the Configuration page. Operators and viewers can not access the configuration page. Though operators can not access the page, they are capable of using the url commands to get and set the value of parameters. For more information, please refer to URL Commands of the Network Camera on page 56. Viewers can only access the main page.

Manage User



Manage User

User name:

User password:

User type:

○ Administrator
○ Operator
○ Viewer

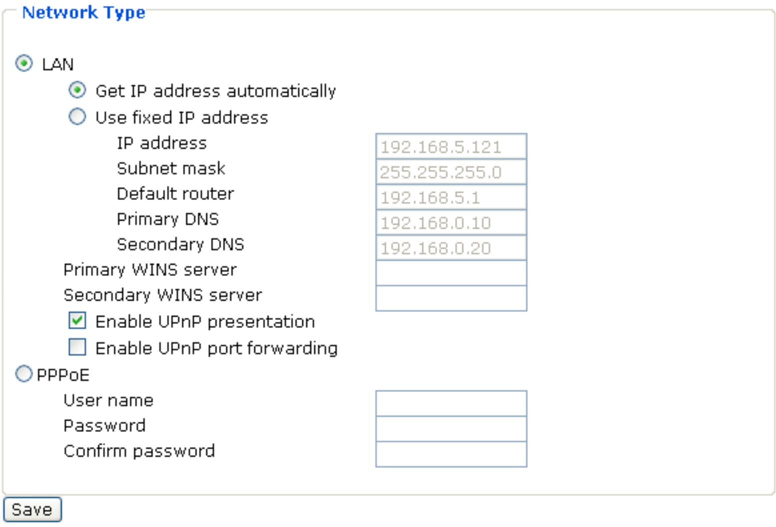
Here you can change user’s access rights or delete user accounts.

1. Pull down the user list to find an account.
2. Make necessary changes and then click **Save** or **Delete** to enable the settings.

Network

This section explains how to configure wired network connection for the Network Camera. It is composed of the following five columns: Network Type, HTTP, Two way audio, FTP and RTSP Streaming. When completed with the settings on this page, click **Save** to enable the settings.

Network Type



Network Type

● LAN

● Get IP address automatically

○ Use fixed IP address

IP address	192.168.5.121
Subnet mask	255.255.255.0
Default router	192.168.5.1
Primary DNS	192.168.0.10
Secondary DNS	192.168.0.20
Primary WINS server	
Secondary WINS server	

☑ Enable UPnP presentation

□ Enable UPnP port forwarding

○ PPPoE

User name	
Password	
Confirm password	

LAN

Select this option when the Network Camera is deployed in a local area network (LAN) and is intended to be accessed by local computers.

Get IP address automatically: Select this option to obtain an available dynamic IP address assigned by a DHCP server each time the camera is connected to the LAN.

Use fixed IP address: Select this option to manually assign a static IP address to the Network Camera. The Network Camera can automatically restart and operate normally after a power outage. Please refer to Internet connection with static IP on page 8 for details.

Subnet mask: This is used to determine if the destination is in the same subnet. The default value is “255.255.255.0”.

Default router: This is the gateway used to forward frames to destinations in a different subnet. Invalid router setting will fail the transmission to destinations in different subnet.

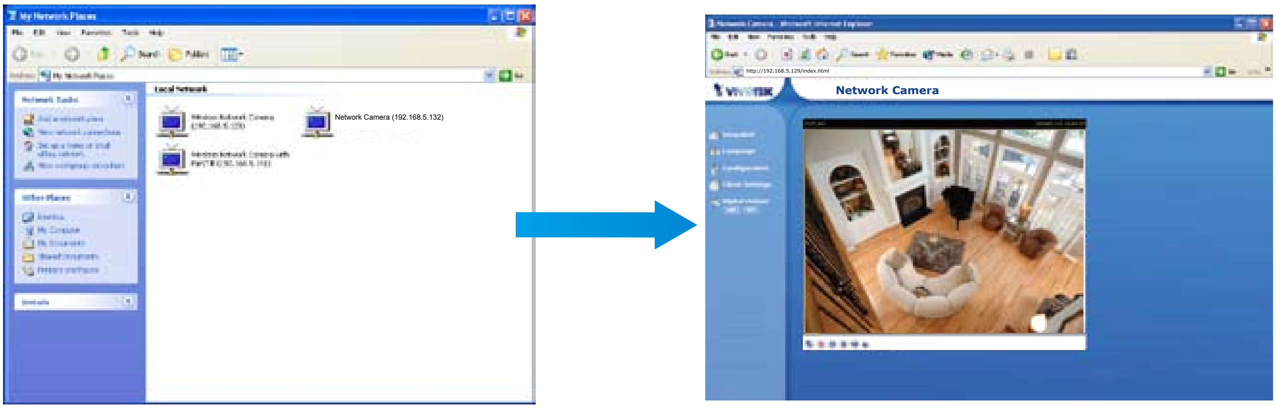
Primary DNS: The primary domain name server that translates hostnames into IP addresses.

Secondary DNS: Secondary domain name server that backups the Primary DNS.

Primary WINS server: The primary WINS server that maintains the database of computer name and IP address.

Secondary WINS server: The secondary WINS server that maintains the database of computer name and IP address.

Enable UPnP presentation: Select this option to enable UPnP^{TM} presentation for your Network Camera so that whenever a Network Camera is presented to the LAN, shortcuts of connected Network Cameras will be listed in My Network Places. Currently, UPnP^{TM} is supported by Windows XP or later. Note that to utilize this feature, please make sure the UPnP^{TM} component is installed on your computer.



Enable UPnP port forwarding: To access the Network Camera from the Internet, select this option to allow the Network Camera to open ports on the router automatically so that video streams can be sent out from a LAN. To utilize of this feature, make sure that your router supports UPnP^{TM} and it is activated.

PPPoE (Point-to-point over Ethernet)

Select this option to configure your Network Camera to make it accessible from anywhere as long as there is an Internet connection. Note that to utilize this feature, it requires an account provided by your ISP.

Follow the steps below to acquire your Network Camera's public IP address.

1. Set up the Network Camera in LAN.
2. Go to Configuration > Application > Server Settings (please refer to Server Settings on page 45) to add a new server -- email or FTP server.
3. Go to Configuration > Application > Media Settings (please refer to Media Settings on page 43). Select System log so that you will receive a list of system log in TXT file format which contains the Network Camera's public IP address in your email or on the FTP server.
4. Go to Configuration > Network > Network Type. Select PPPoE and enter the user name and password provided by your ISP. Click Save to enable the settings.
5. The Network Camera starts to reboot.
6. Disconnect the power source of the Network Camera; remove it from the LAN environment to the Internet.

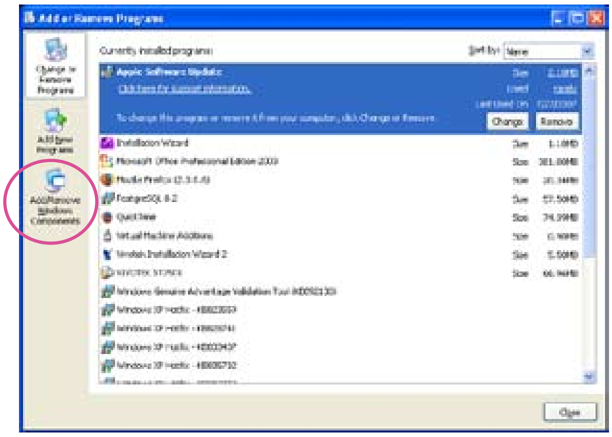
NOTE

► *If the default ports are already used by other device connecting to the same router, the Network Camera will select other ports for the Network Camera.*

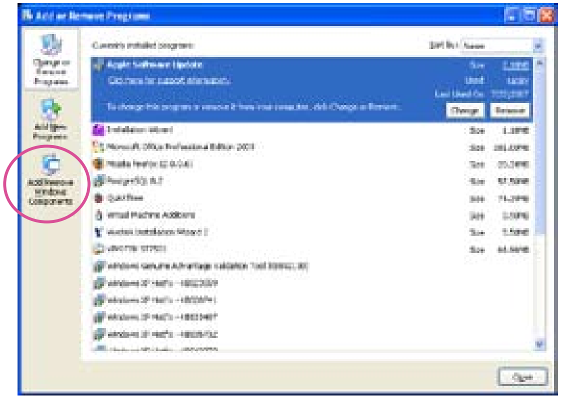
► *If UPnP^{TM} is not supported by your router, you will see the following message:*
Error: Router does not support UPnP port forwarding.

► *Steps to enable UPnP™ user interface on your computer:*
Note that you must log on to the computer as a system administrator to install the UPnP™ components.

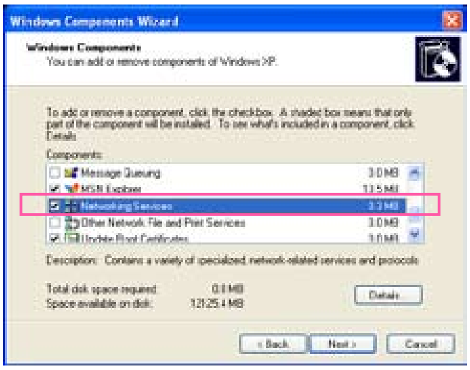
1. Go to Start, click Control Panel, and then click Add or Remove Programs.



2. In the Add or Remove Programs dialog box, click Add/Remove Windows Components.


Add or Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Currently installed programs:
Apple Software Update
Change
Remove
Close

3. In the Windows Components Wizard dialog box, select Networking Services and then click Details.



Windows Components Wizard

Windows Components
You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

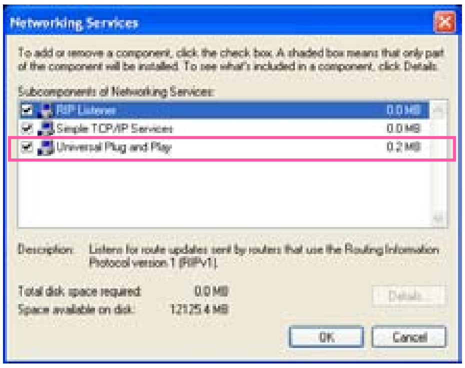
Components:

□	Message Queuing	3.0 MB
☑	MSN Explorer	13.5 MB
☑	Networking Services	3.3 MB
□	Other Network File and Print Services	3.0 MB
☑	Update Root Certificates	1.0 MB

Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 0.0 MB
Space available on disk: 12125.4 MB

4. In the Networking Services dialog box, select Universal Plug and Play and then click OK.



Networking Services

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

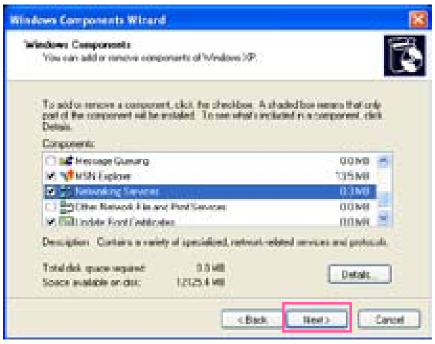
Subcomponents of Networking Services:

☑	RIP Listener	0.0 MB
☑	Simple TCP/IP Services	0.0 MB
☑	Universal Plug and Play	0.2 MB

Description: Listens for route updates sent by routers that use the Routing Information Protocol version 1 (RIPV1).

Total disk space required: 0.0 MB
Space available on disk: 12125.4 MB

5. Click Next in the following window.



Windows Components Wizard

Windows Components
You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☐ Message Queuing 0.0 MB
☑ MSN Explorer 13.5 MB
☑ Networking Services 0.3 MB
☐ Other Network File and Print Services 0.0 MB
☑ Update Root Certificates 0.0 MB

Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 0.0 MB
Space available on disk: 12125.4 MB

6. Click Finish. UPnP™ is enabled.

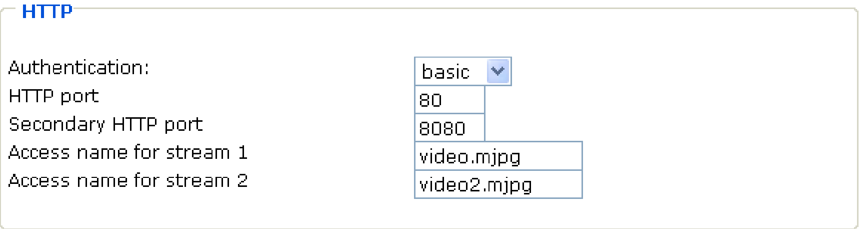
► *How does UPnP™ work?*
UPnP™ networking technology provides automatic IP configuration and dynamic discovery of devices added to a network. Services and capabilities offered by networked devices, such as printing and file sharing, are available among each other without bothersome network configuration. In the case of Network Cameras, you will see Network Camera shortcuts at My Network Places.

► *Enabling UPnP port forwarding allows the Network Camera to open secondary HTTP port on the router, not HTTP port, meaning that you have to add the secondary HTTP port number behind the Network Camera's public address in order to access the Network Camera from the Internet. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.*

From the Internet	In LAN
http://203.67.124.123:8080	http://192.168.4.160 or http://192.168.4.160:8080

► *If the PPPoE settings are incorrectly configured or the Internet access is not working, restore the Network Camera to factory default; please refer to Restore on page 52 for details. After the Network Camera is reset to factory default, it is accessible in LAN.*

HTTP

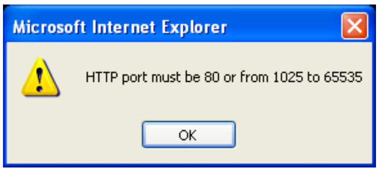


HTTP

Authentication: basic
HTTP port 80
Secondary HTTP port 8080
Access name for stream 1 video.mjpg
Access name for stream 2 video2.mjpg

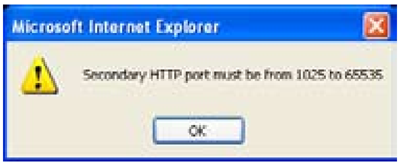
Authentication: Depending on your network security requirements, the Network Camera provides two types of security settings for a HTTP transaction: basic and digest. If basic authentication is selected, the password is sent in plain text format; there can be potential risks of being intercepted. If digest authentication is selected, user credentials are encrypted in MD5 algorithm and thus provide better protection against unauthorized accesses.

HTTP port / Secondary HTTP port: By default, the HTTP port is set to 80 and the secondary HTTP port is set to 8080. Also, they can be assigned with another port number between 1025 and 65535. If the ports are incorrectly assigned, the following warning messages are displayed:



Microsoft Internet Explorer

HTTP port must be 80 or from 1025 to 65535



Microsoft Internet Explorer

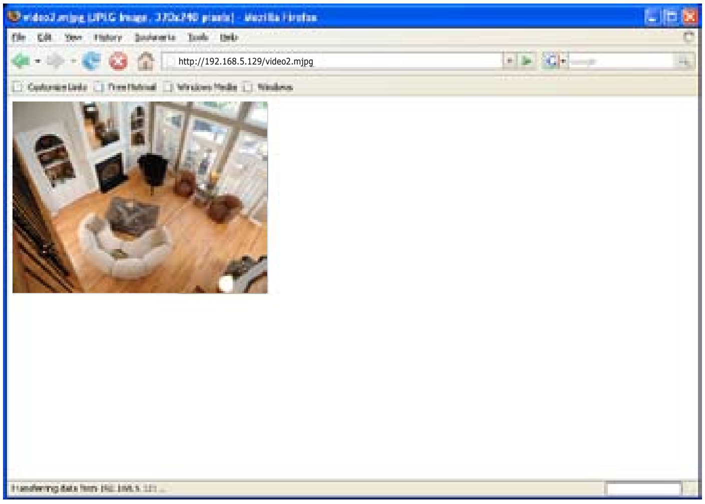
Secondary HTTP port must be from 1025 to 65535

To access the Network Camera within LAN, both HTTP port and secondary HTTP port can be used to access the Network Camera. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.

In LAN
http://192.168.4.160 or http://192.168.4.160:8080

Access name for stream 1 / Access name for stream 2: The access name is used to differentiate the streaming source. When using Mozilla Firefox or Netscape to access the Network Camera, and the video mode is set to JPEG, users will receive continuous JPEG pictures. This technology, known as "server push", allows the Network Camera to feed live pictures to Mozilla Firefox and Netscape.
Use http://<ip address>:<http port>/<access name for stream1 or stream2> to make connection.

For example, when the access name for stream 2 is set to video.mjpg:
1. Launch Mozilla Firefox or Netscape.
2. Type the URL command in the address field. Press Enter.
3. The JPEG images will be displayed in your web browser.



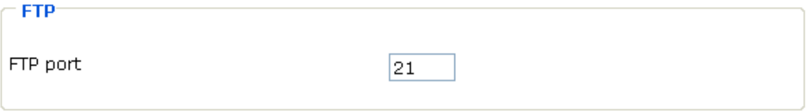
http://192.168.5.129/video2.mjpg

NOTE

► *To utilize the HTTP authentication, make sure that your have set a password for the Network Camera first; please refer to Security on page 22 for details.*

► *Microsoft® Internet Explorer does not support server push technology; therefore, using http://<ip address>:<http port>/<access name for stream1 or stream2> will fail to access the Network Camera.*

FTP

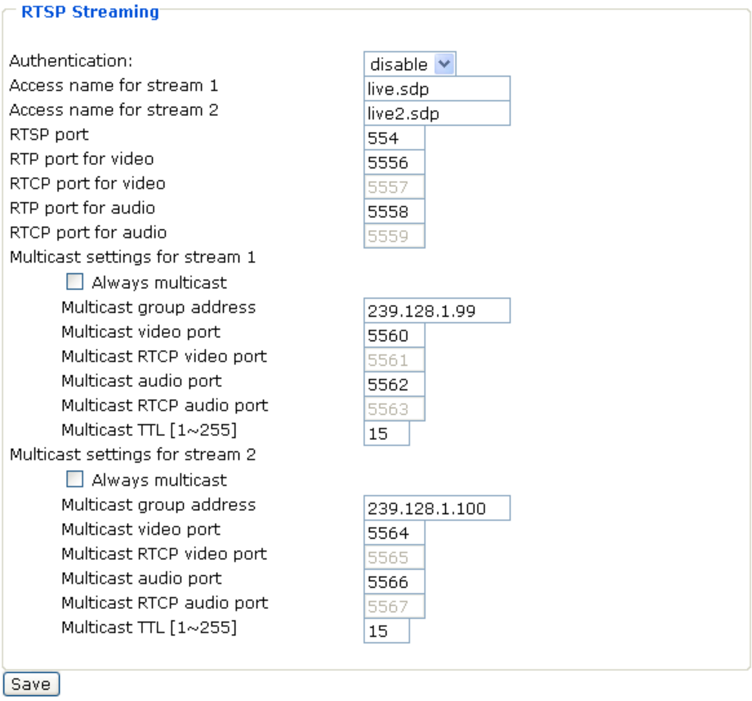


FTP

FTP port 21

The FTP server allows the Network Camera to utilize VIVOTEK Installation Wizard 2 to upgrade firmware. By default, the FTP port is set to 21. Also, it can be assigned with another port number between 1025 and 65535.

RTSP Streaming



RTSP Streaming

Authentication:	disable
Access name for stream 1	live.sdp
Access name for stream 2	live2.sdp
RTSP port	554
RTP port for video	5556
RTCP port for video	5557
RTP port for audio	5558
RTCP port for audio	5559
Multicast settings for stream 1	
□ Always multicast	
Multicast group address	239.128.1.99
Multicast video port	5560
Multicast RTCP video port	5561
Multicast audio port	5562
Multicast RTCP audio port	5563
Multicast TTL [1~255]	15
Multicast settings for stream 2	
□ Always multicast	
Multicast group address	239.128.1.100
Multicast video port	5564
Multicast RTCP video port	5565
Multicast audio port	5566
Multicast RTCP audio port	5567
Multicast TTL [1~255]	15

Authentication: Depending on your network security requirements, the Network Camera provides three types of security settings for streaming via RTSP protocol: disable, basic and digest. If basic authentication is selected, the password is sent in plain text format; there can be potential risks of being intercepted. If digest authentication is selected, user credentials are encrypted in MD5 algorithm and thus provide better protection against unauthorized accesses.

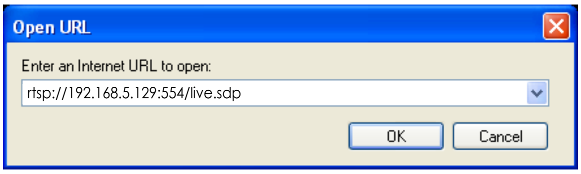
The accessibility of the RTSP streaming for the three authentication modes are listed in the following table:

	Quick Time player	Real Player
Disable	O	O
Basic	O	O
Digest	O	X

O indicates that the authentication mode is supported by the RTSP player.
X indicates that the authentication mode is NOT supported by the RTSP player.

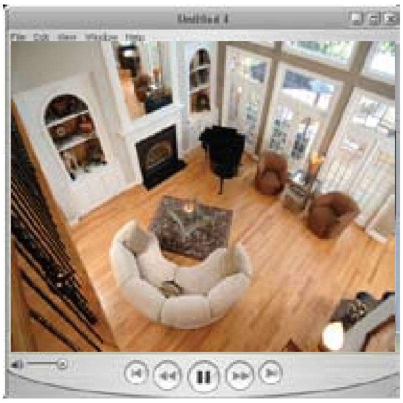
Access name for stream 1 / Access name for stream 2: The access name is used to differentiate the streaming source. When using a RTSP player to access the Network Camera, and the video mode is set to MPEG-4, use the following RTSP URL command to request a transmission of streaming data.

rtsp://<ip address>:<rtsp port>/<access name for stream1 or stream2>
For example, when the access name for stream 1 is set to live.sdp:
1. Launch a RTSP player.
2. Choose File > Open URL. An URL dialog box will pop up.
3. Type the URL command in the text box.
   For example:



Enter an Internet URL to open:
rtsp://192.168.5.129:554/live.sdp

4. The live video will be displayed in your player.



RTSP port /RTP port for video, audio/ RTCP port for video, audio

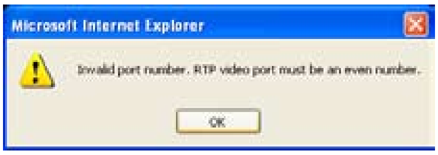
The RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media. By default, the port number is set to 554.

The RTP (Real-time Transport Protocol) is used to deliver video and audio data to the clients. By default, the RTP port for video is set to 5556 and the RTP port for audio is set to 5558.

The RTCP (Real-time Transport Control Protocol) allows the Network Camera to transmit the data by monitoring Internet traffic volume. By default, the RTCP port for video is set to 5557 and the RTCP port for audio is set to 5559.

The five ports can be changed between 1025 and 65535. The RTP port must be an even number and the RTCP port is RTP port number plus one, and thus always be odd. When the RTP port changes, the RTCP port will change accordingly.

If the RTP ports are incorrectly assigned, the following warning message is displayed:

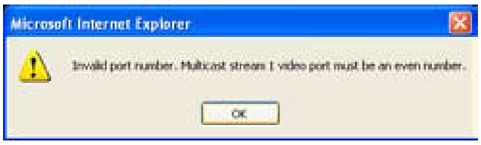

Microsoft Internet Explorer

Invalid port number. RTP video port must be an even number.

Multicast settings for stream 1 / Multicast settings for stream 2: Select the Always multicast to enable multicast for stream 1 or stream 2. Unicast video transmission delivers a stream through point-to-point transmission; multicast, on the other hand, sends a stream to the multicast group address and allows multiple clients to acquire the stream by requesting a copy from the Multicast group address.

The five ports can be changed between 1025 and 65535. The multicast RTP port must be an even number and the multicast RTCP port number is the multicast RTP port number plus one, and thus it is always be odd. When the multicast RTP port changes, the multicast RTCP port will change accordingly.

If the multicast RTP video ports are incorrectly assigned, the following warning message is displayed:


Microsoft Internet Explorer

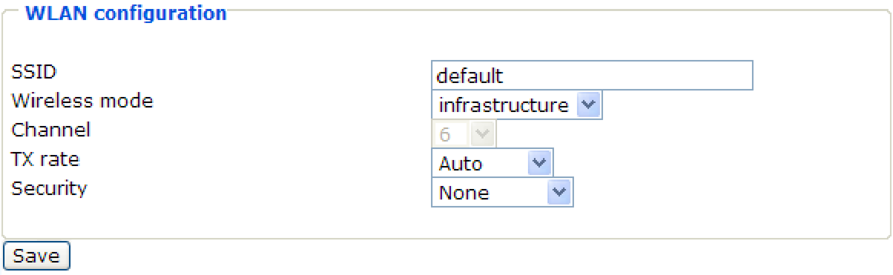
Invalid port number. Multicast stream 1 video port must be an even number.

Multicast TTL [1~255]:The multicast TTL (Time to live) is the value that tells the router the range a packet can be forwarded.

NOTE

► *To utilize the RTSP streaming authentication, make sure that your have set a password for the Network Camera first; please refer to Security on page 22 for details.*

Wireless LAN (IP7134 only)



WLAN configuration

SSID	default
Wireless mode	infrastructure
Channel	6
TX rate	Auto
Security	None

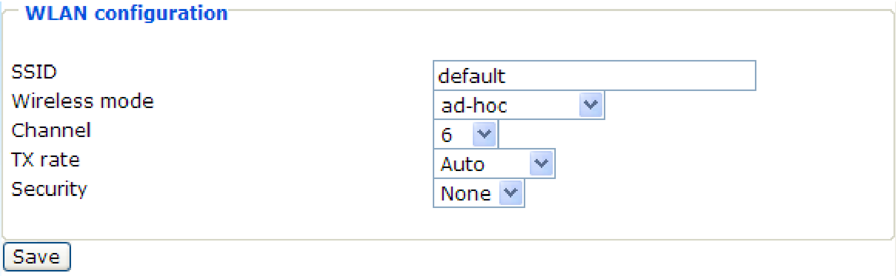
Save

SSID (Service Set Identifier): It is a name that identifies a wireless network. Access Points and wireless clients attempting to connect to a specific WLAN (Wireless Local Area Network) must use the same SSID. The default setting is default. Note: The maximum length of SSID is 32 single-byte characters and SSID can't be any of ", <, > and space character.

Wireless mode: Clicking on the pull-down menu to select from the following options:

Infrastructure: Make the Network Camera connect to the WLAN via an Access Point. (The default setting)

Ad-Hoc: Make the Network Camera connect directly to a host equipped with a wireless adapter in a peer-to-peer environment.



WLAN configuration

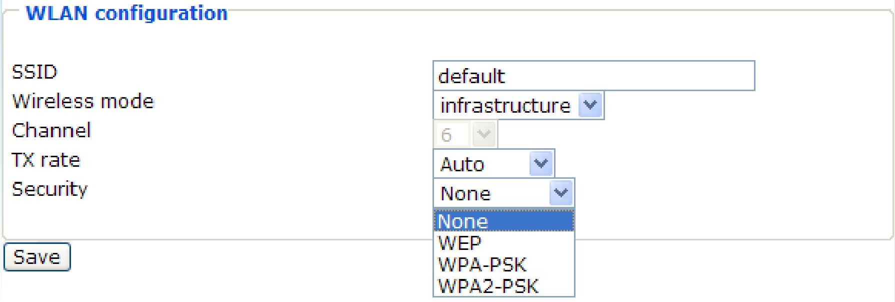
SSID	default
Wireless mode	ad-hoc
Channel	6
TX rate	Auto
Security	None

Save

Channel: While in infrastructure mode, the channel is selected automatically to match the channel setting for the selected Access Point. In Ad-Hoc mode, the channel must be manually set to the same channel for each wireless adapter. The default channel setting depends on the installed region.

TX rate: This field is for selecting the maximum transmission rate on the network. The default setting is "auto", that is the Network Camera will try to connect to the other wireless device with highest transmitting rate.

Security: Select the data encrypt method. There are four types from low to high: none, WEP, WPA-PSK, and WPA2-PSK.

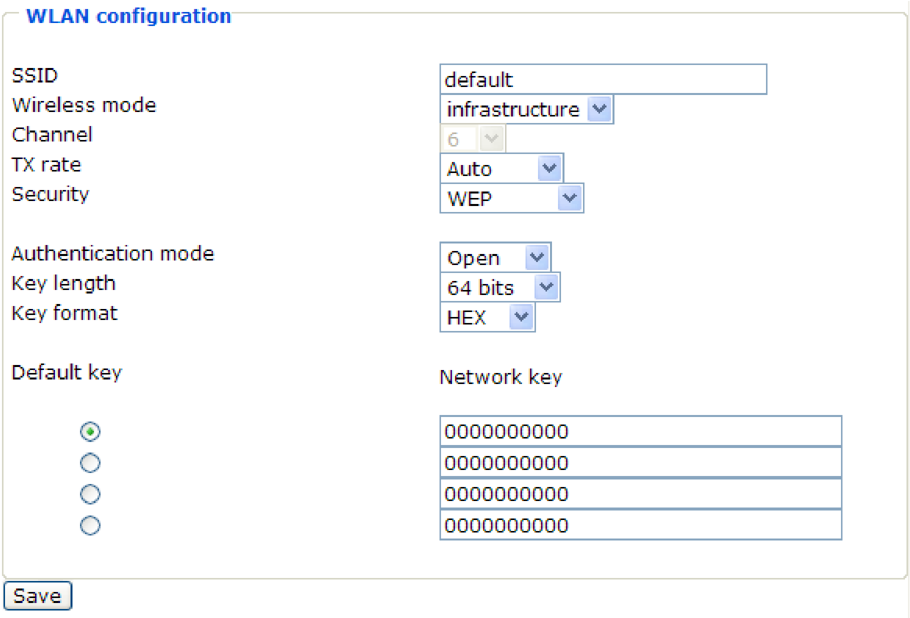


WLAN configuration

SSID	default
Wireless mode	infrastructure
Channel	6
TX rate	Auto
Security	None

1. None: No data encryption.

2. WEP (Wired equivalent Privacy): It allows communication only with other devices with identical WEP settings.



WLAN configuration

SSID	default
Wireless mode	infrastructure
Channel	6
TX rate	Auto
Security	WEP
Authentication mode	Open
Key length	64 bits
Key format	HEX
Default key	Network key
●	0000000000
○	0000000000
○	0000000000
○	0000000000

■ Authentication Mode: Choose one of the following modes. Open is the default setting.
Open – communicates the key across the network.
Shared – allows communication only with other devices with identical WEP settings.

■ Key length: The administrator can select the key length among 64 or 128 bits.
64 bits is the default setting.

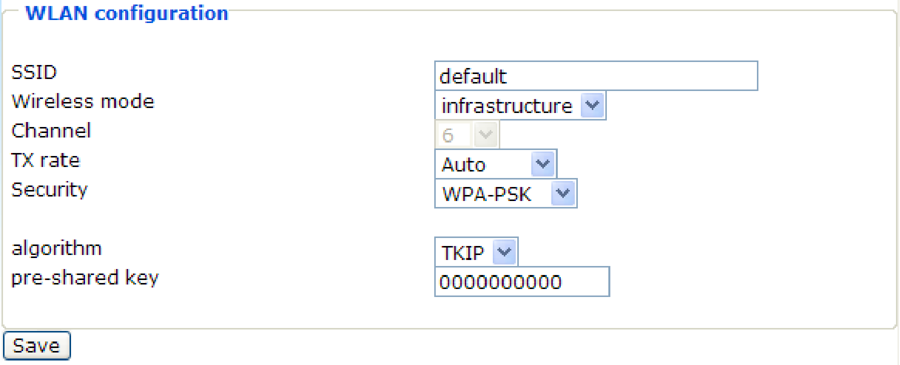
■ Key format: Hexadecimal or ASCII. HEX is the default setting.
HEX digits consist of the numbers 0~9 and the letters A-F.
ASCII is a code for representing English letters as numbers from 0-127 except “, <, > and space characters that are reserved.

■ Network Key: Enter a key in either hexadecimal or ASCII format.
You can select different key length, and acceptable input length is listed as following:
64 bits key length: 10 Hex digits or 5 characters.
128 bites key length: 26 Hex digits or 13 characters.

NOTE

► *When 22(“), 3C(<) or 3E(>) are input in network key, the key format can’t be changed to ASCII format.*

3. WPA-PSK: Use WPA (Wi-Fi Protected Access) pre-shared key.



SSID	default
Wireless mode	infrastructure
Channel	6
TX rate	Auto
Security	WPA-PSK
algorithm	TKIP
pre-shared key	0000000000

More secure than WEP, the Wi-Fi Alliance developed WPA (Wi-Fi Protected Access) in 2003 to address WEP's weaknesses. Improvements included TKIP, which changes the encryption key for each data transmission.

■ Algorithm: Choosing one of the following algorithm for WPA-PSK and WPA2-PSK modes.

TKIP (Temporal Key Integrity Protocol): A security protocol used in the IEEE 802.11 wireless networks. TKIP is a "wrapper" that goes around the existing WEP encryption. TKIP comprises the same encryption engine and RC4 algorithm defined for WEP. However, the key used for encryption in TKIP is 128 bits long. This solves the first problem of WEP: a too-short key length. (From Wikipedia)

AES (Advanced Encryption Standard): In cryptography, the Advanced Encryption Standard (AES), also known as Rijndael, is a block cipher adopted as an encryption standard by the U.S. government. As of 2006, AES is one of the most popular algorithms used in symmetric key cryptography. (From Wikipedia)

■ Pre-shared Key: Entering a key in ASCII format. The length of the key is 8 ~ 63.

4. WPA2-PSK: Use WPA2 pre-shared key.

The advanced protocol, certified through Wi-Fi Alliance's WPA2 program, implements the mandatory elements of 802.11i. In particular, it introduces a new AES-based algorithm, CCMP, that is considered fully secure. From March 13, 2006, WPA2 certification is mandatory for all new devices wishing to be certified by the Wi-Fi Alliance as "Wi-Fi CERTIFIED." (From Wikipedia)

NOTE

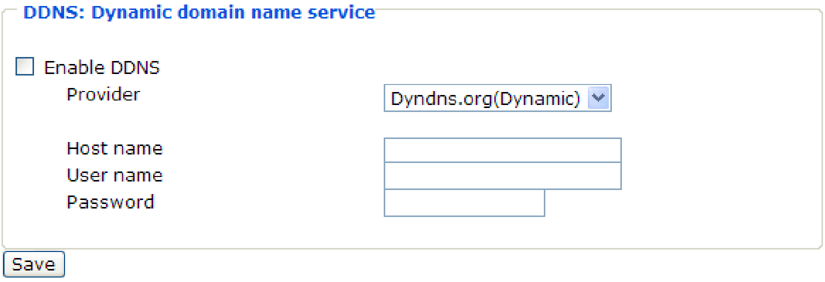
► *After wireless configurations are completed, click Save and the camera will reboot. Wait for the live image is reloaded to your browser. For VIVOTEK 7000-series cameras, you have to unplug the power cable and Ethernet cable from the camera; then re-plug the power cable to the camera. The camera will switch to wireless mode.*

► *Some invalid settings may cause the system failing to respond. Change the Configuration only if necessary and consult with your network supervisor or experienced users for correct settings. Once the system has lost contact, refer to Appendix A for reset and restore procedures.*

DDNS

This section explains how to configure dynamic domain name service for the Network Camera. DDNS is a service that allows your Network Camera, especially when assigned with a dynamic IP address, to have a fixed host and domain name.

DDNS: Dynamic domain name service



DDNS: Dynamic domain name service

□ Enable DDNS

Provider: Dyndns.org(Dynamic)

Host name

User name

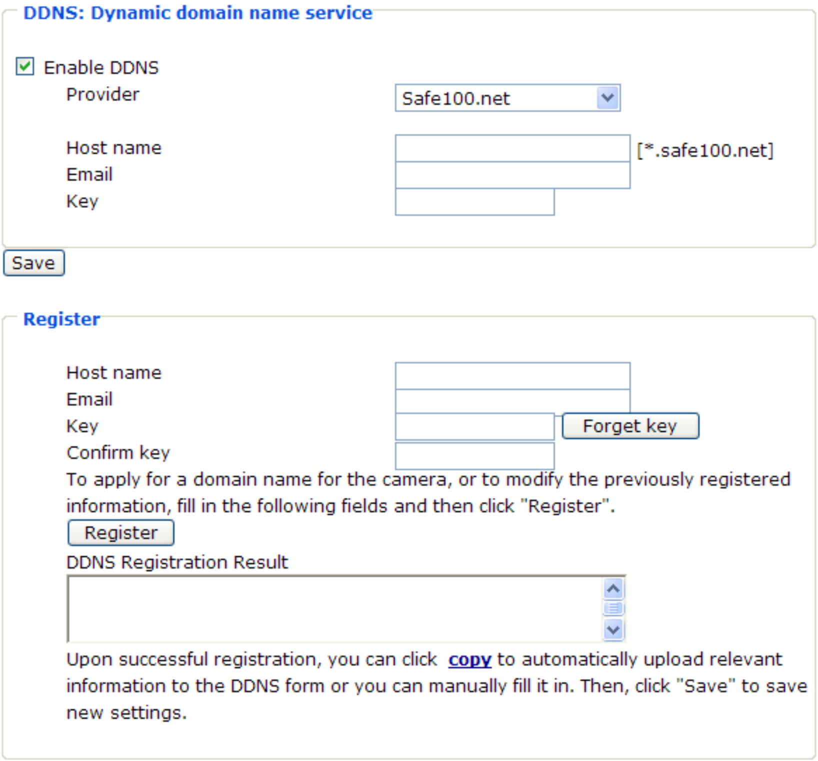
Password

Enable DDNS: Select this option to enable the DDNS setting.

Provider: Select a DDNS provider of your choice from the Provider drop-down list.
VIVOTEK offers safe100, a free dynamic domain name service to VIVOTEK customers. It is recommended that you register with the safe100 to access the Network Camera from the Internet. Additionally, we offer other DDNS providers, such as Dyndns.org(Dynamic), Dyndns.org(Custom), TZO.com, DHS.org, CustomSafe100, dyn-interfree.it. Note that to utilize this feature, please apply a dynamic domain account first.

■ Safe100.net

1. In the DDNS column, select Safe100 from the Provider drop-down list. Click Agree when you agree with the terms of the Service Agreement.
2. In the Register column, fill in the Host name, Email, Key and Confirm Key and then click Register. After a host name has been successfully created, you will see a successful message in the DDNS Registration Result column, indicating that you have successfully applied a domain name on Safe100.net.



DDNS: Dynamic domain name service

☑ Enable DDNS

Provider: Safe100.net

Host name [*.safe100.net]

Email

Key

Register

Host name

Email

Key

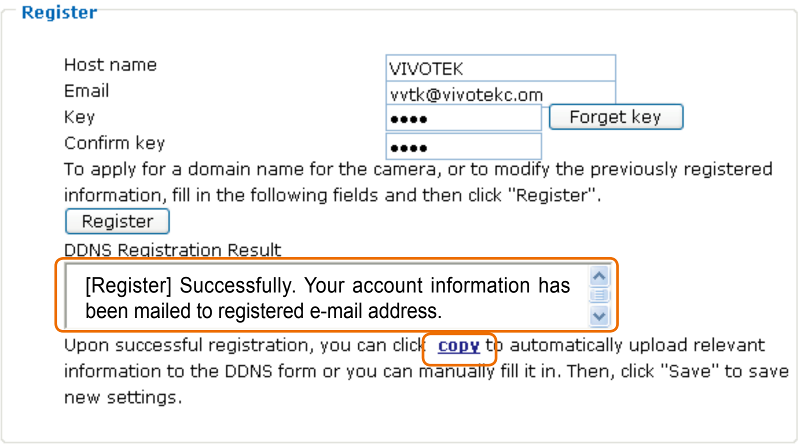
Confirm key

To apply for a domain name for the camera, or to modify the previously registered information, fill in the following fields and then click "Register".

DDNS Registration Result

Upon successful registration, you can click copy to automatically upload relevant information to the DDNS form or you can manually fill it in. Then, click "Save" to save new settings.

3. Click Copy and all the registered information will be uploaded to the corresponding fields in the DDNS column.



Register

Host name VIVOTEK
Email vvtk@vivotekc.om
Key ●●●●
Confirm key ●●●●

To apply for a domain name for the camera, or to modify the previously registered information, fill in the following fields and then click "Register".

DDNS Registration Result

[Register] Successfully. Your account information has been mailed to registered e-mail address.

Upon successful registration, you can click copy to automatically upload relevant information to the DDNS form or you can manually fill it in. Then, click "Save" to save new settings.

4. Select Enable DDNS and then click Save to enable the settings.

■ CustomSafe100

VIVOTEK offers documents to establish CustomSafe100 DDNS server for distributors and system integrators. You can use CustomSafe100 to register a dynamic domain name if your distributor or system integrators offer such services.

1. In the DDNS column, select CustomSafe100 from the Provider drop-down list.
2. In the Register column, fill in the Host name, Email, Key and Confirm Key; then click **Register**.
   After a host name has been successfully created, you will see a successful message in the DDNS Registration Result column, indicating that you have successfully registered a domain name on CustomSafe100.
3. Click **Copy** and all the registered information will be uploaded to the corresponding fields in the DDNS column.
4. Select Enable DDNS and then click **Save** to enable the settings.

Forget key: Click this button if you forget the key of Safe100 or CustomSafe100. Your account information will be sent to your email address.

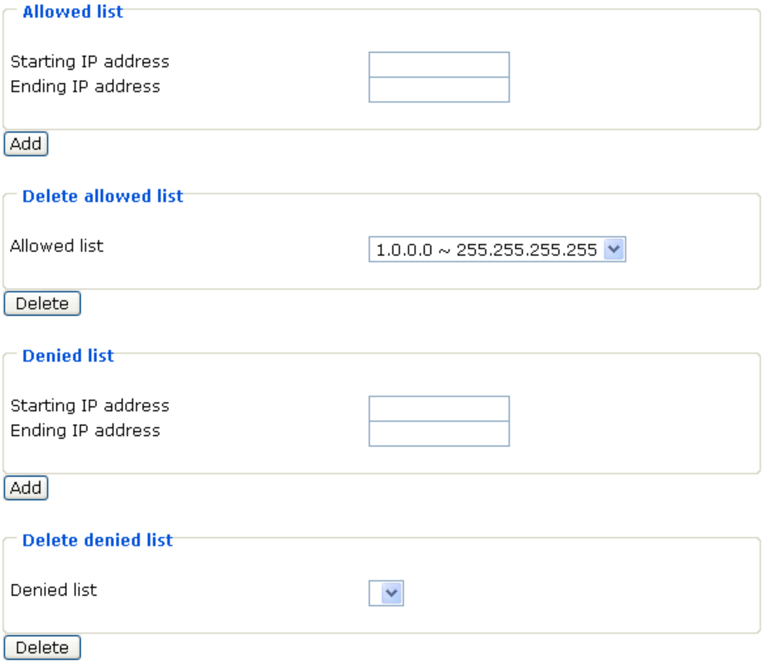
Refer to the following links to apply a dynamic domain account when selecting other DDNS providers:

■ Dyndns.org(Dynamic) / Dyndns.org(Custom): visit http://www.dyndns.com/
■ TZO.com: visit http://www.tzo.com/
■ DHS.org: visit http://www.dhs.org/
■ dyn-interfree.it: visit http://dyn-interfree.it/

Access list

This section explains how to control the access permission by checking the client PC's IP addresses. It is composed of the following four columns: Allowed list, Denied list, Delete allowed list, and Delete denied list.

Allowed list / Denied list



Allowed list

Starting IP address

Ending IP address

Add

Delete allowed list

Allowed list 1.0.0.0 ~ 255.255.255.255

Delete

Denied list

Starting IP address

Ending IP address

Add

Delete denied list

Denied list

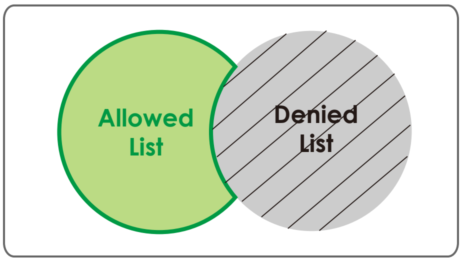
Delete

There are two lists for permission control: Allowed list and Denied list. Only those clients whose IP addresses are in the Allowed list and not in the Denied list can access the Network Camera.

1. In the Allowed list or Denied list column, type the starting IP address and ending IP address in the text boxes. A total of ten lists can be configured for both columns.
2. Click Add to enable the settings.

NOTE

► *For example, when the range of allowed list is set from 1.1.1.0 to 192.255.255.255 and the range of denied list is set from 1.1.1.0 to 170.255.255.255, Only users' IP located between 171.0.0.0 and 192.255.255.255 can access the Network Camera.*



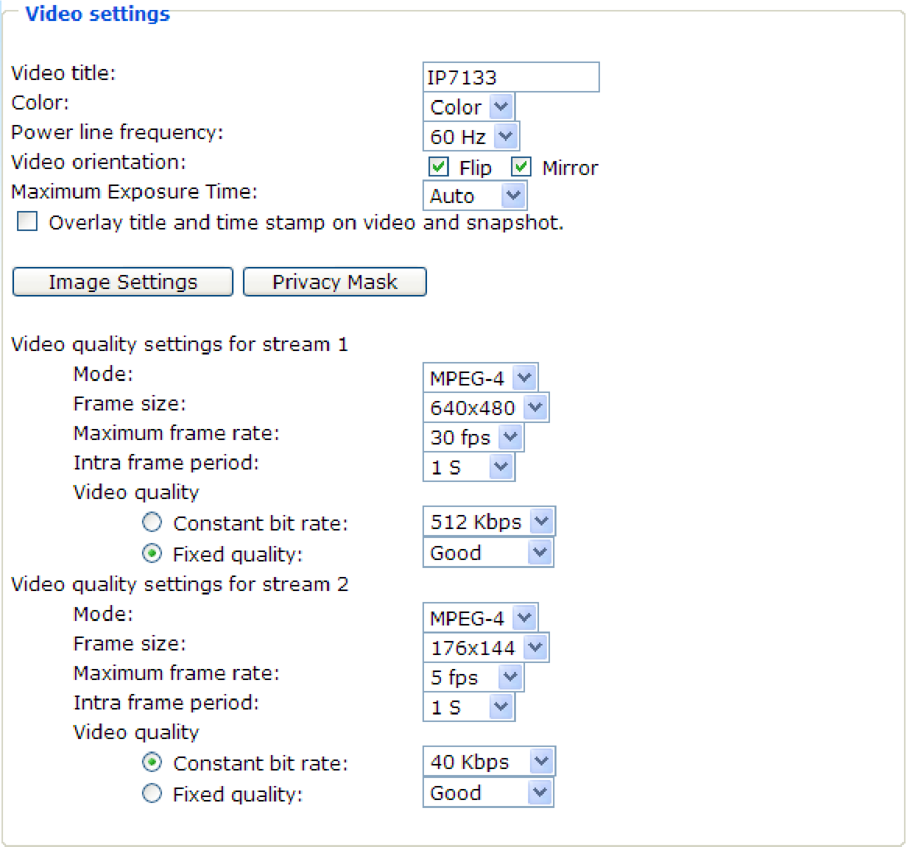
Delete allowed list / Delete denied list

1. In the Delete allowed list or Delete denied list, select a list from the drop-down list.
2. Click **Delete** to enable the settings.

Audio and video

This section explains how to cofigure audio and video performances of the Network Camera. It is composed of the following two columns: Video settings and Audio settings.

Video settings



Video settings

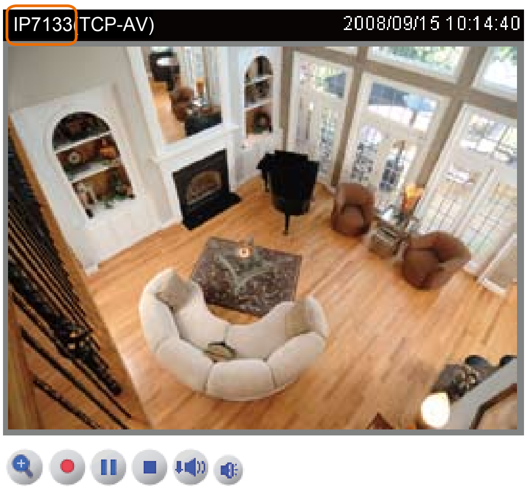
Video title:	IP7133
Color:	Color
Power line frequency:	60 Hz
Video orientation:	☑ Flip ☑ Mirror
Maximum Exposure Time:	Auto

□ Overlay title and time stamp on video and snapshot.

Image Settings | Privacy Mask

Video quality settings for stream 1	
Mode:	MPEG-4
Frame size:	640x480
Maximum frame rate:	30 fps
Intra frame period:	1 S
Video quality	
○ Constant bit rate:	512 Kbps
● Fixed quality:	Good
Video quality settings for stream 2	
Mode:	MPEG-4
Frame size:	176x144
Maximum frame rate:	5 fps
Intra frame period:	1 S
Video quality	
● Constant bit rate:	40 Kbps
○ Fixed quality:	Good

Video title: Enter a name that will be displayed on the title bar of the live video.



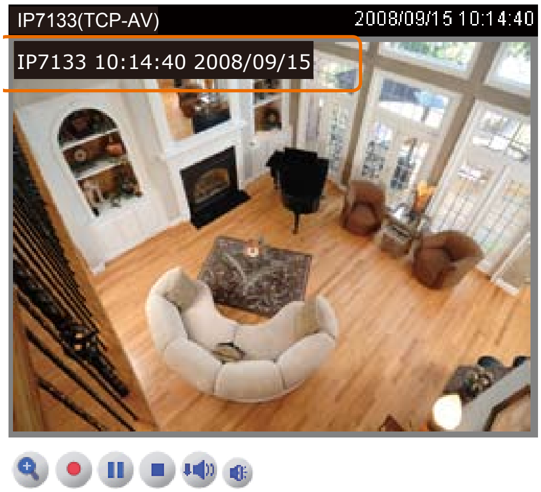
Color: Select to display colorful or black/white video streams.

Power line frequency: Set the power line frequency in consistent with local utility settings to eliminate uncomfortable image flickering associated with fluorescent lights. Note that after the power line frequency is changed, it is required to disconnect and reconnect the power cord of the Network Camera in order for the new setting to enable the settings.

Video orientation: Flip--vertically reflect the display of the live video; Mirror--horizontally reflect the display of the live video. Select both options if the Network Camera is installed upside-down (ex. on the ceiling) to correct the image orientation.

Maximum Exposure Time: 1/30 S, 1/15 S, and Auto.

Overlay title and time stamp on video: Select this option to place the video title and time on video streams.
Note that when the frame size is set to 176 x 144 as the right picture below, only time will be stamped on video streams.



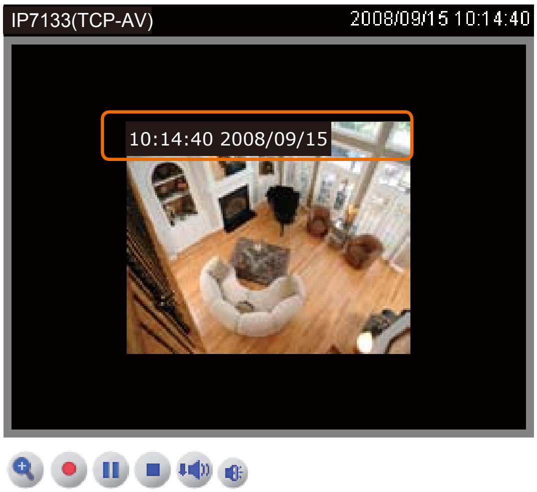
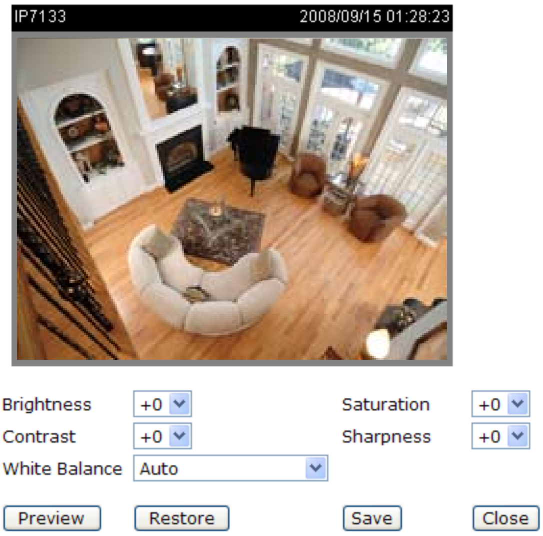


Image Settings

Click Image settings to open the Image Settings page. On this page, you can tune White balance, Brightness, Saturation, Contrast, and Sharpness for video compensation.



Brightness +0

Saturation +0

Contrast +0

Sharpness +0

White Balance Auto

- Brightness: Adjust the image brightness level, which ranges from -5 to +5. The default value is set to 0.
- Saturation: Adjust the image saturation level, which ranges from -5 to +5. The default value is set to 0.
- Contrast: Adjust the image contrast level, which ranges from -5 to +5. The default value is set to 0.
- Sharpness: Adjust the image sharpness level, which ranges from -3 to +3. The default value is set to +3.

White balance: Adjust the value for best color temperature.

■ Auto

The Network Camera automatically adjusts the color temperature of light in response to different light sources. The white balance setting defaults to Auto and works well in most situations.

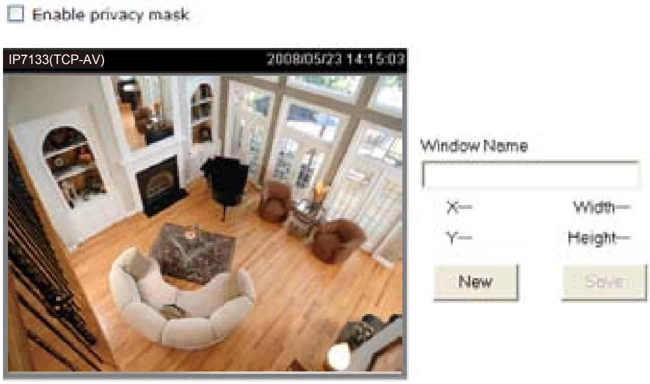
■ Keep current value

Follow the steps below to manually set the white balance to compensate for the ambient lighting conditions.

1. Set the White balance to Auto and click Save.
2. Place a sheet of white paper in front of the lens; then allow the Network Camera to adjust the color temperature automatically.
3. Select Keep current value to confirm the setting while the white balance is being measured.
4. Click Save to enable the settings.

Privacy mask

Click Privacy Mask to open the Privacy Mask page. On this page, you can block out some sensitive zones for privacy concerns.

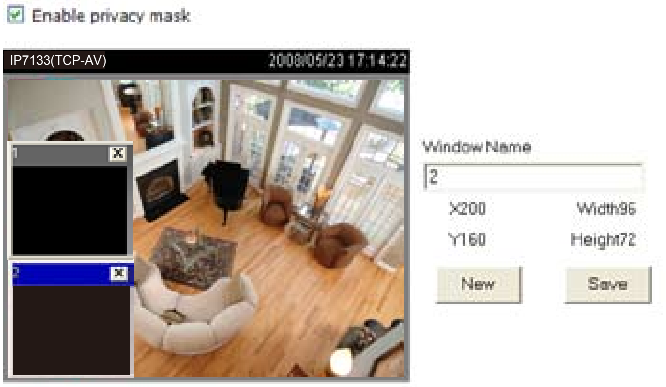


☐ Enable privacy mask

Window Name

X-- Width--

Y-- Height--



☑ Enable privacy mask

Window Name 2

X200 Width96

Y160 Height72

■ To set the privacy mask windows, follow the steps below:

1. Click New to add a new window.
2. To resize and drag-drop the window, which is recommended to be at least twice the size of the object (height and width) you want to cover.
3. Enter a descriptive Window Name and click Save to enable the settings.
4. Select Enable privacy mask to enable this function.

NOTE

► *Up to 5 privacy mask windows can be set in the same screen.*

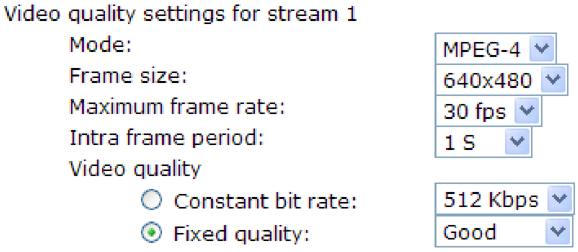
► *If you want to delete the window, please click on the 'x' at the upper right-hand corner of the window to close the window.*

Video quality settings for stream 1 / stream 2: You can set up two seperate streams for the Network Camera for different viewing devices. For example, set the Network Camera to a smaller frame size and a lower bit rate for remote viewing on mobile phones. Or, set the Network Camera to a larger video size and a higher bit rate for live viewing on web browsers.

■ Mode

The Network Camera offers two choices of video compression standards for real-time viewing: MPEG-4 and MJPEG.

If MPEG-4 mode is selected, it is streamed in RTSP protocol. There are four dependent parameters provided in MPEG-4 mode for video performance adjustment.



Video quality settings for stream 1

Mode:	MPEG-4
Frame size:	640x480
Maximum frame rate:	30 fps
Intra frame period:	1 S
Video quality	
○ Constant bit rate:	512 Kbps
● Fixed quality:	Good

■ Frame size
Select the video size. Note that a larger frame size takes up more bandwidth. The frame sizes are selectable in the following resolutions: 176 x 144, 352 x 240, and 640 x 480.

■ Maximum frame rate
This limits the maximal refresh frame rate per second. Set the frame rate higher for a smoother video quality.

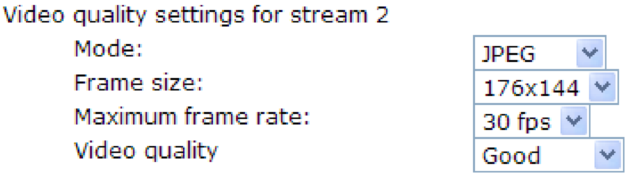
If the power line frequency is set to 50Hz, the frame rates are selectable at the following rates: 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps and 25fps. If the power line frequency is set to 60Hz, the frame rates are selectable at the following rates: 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps, and 30fps.

■ Intra frame period
Determine how often to plant an I frame. The shorter the duration, the more likely you will get a better video quality, but at the cost of higher network bandwidth consumption. Select the intra frame period from the following duration: 1/4 second, 1/2 second, 1 second, 2 seconds, 3 seconds, and 4 seconds.

■ Video quality
A complex scene generally produces larger file size, meaning that higher bandwidth will be needed for data transmission. Therefore, if Constant bit rate is selected, the bandwidth utilization is fixed at a selected level, resulting in mutable video quality performances. The bit rates are selectable at the following rates: 20Kbps, 30Kbps, 40Kbps, 50Kbps, 64Kbps, 128Kbps, 256Kbps, 512Kbps, 768Kbps, 1Mbps, 1.5Mbps, 2Mbps, 3Mbps, and 4Mbps.

On the other hand, if Fixed quality is selected, all frames are transmitted with the same quality; bandwidth utilization is therefore unpredictable. The video qualities are selectable at the following settings: Medium, Standard, Good, Detailed, and Excellent.

If JPEG mode is selected, the Network Camera continuously sends JPEG images to the clients, producing dynamic effects similar to movies. Every single JPEG image transmitted guarantees the same image quality, which in turn comes at the expense of variable bandwidth usage. And because the media contents are a combination of JPEG images, no audio data is transmitted to the clients.



Video quality settings for stream 2

Mode:	JPEG
Frame size:	176x144
Maximum frame rate:	30 fps
Video quality	Good

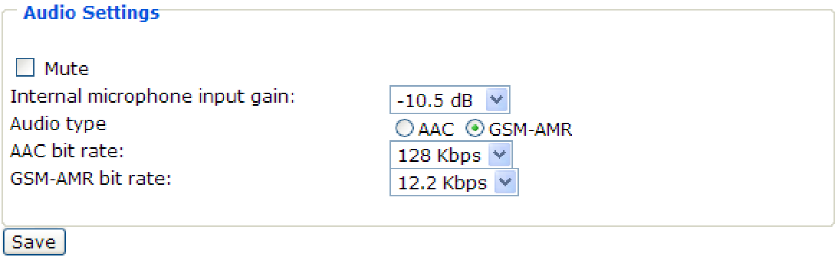
■ Frame size
Select the video size. Note that a larger frame size takes up more bandwidth. The frame sizes are selectable in the following resolutions: 176 x 144, 352 x 240, and 640 x 480.

- ■ Maximum frame rate
  This limits the maximal refresh frame rate per second. Set the frame rate higher for a smoother video quality.

  If the power line frequency is set to 50Hz, the frame rates are selectable at the following rates: 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps and 25fps. If the power line frequency is set to 60Hz, the frame rates are selectable at the following rates: 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps, and 30fps.

- ■ Video quality
  The video qualities are selectable at the following settings: Medium, Standard, Good, Detailed, and Excellent.

Audio settings

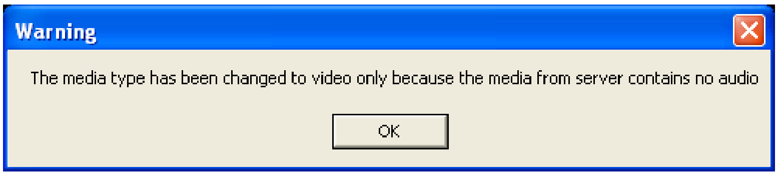


Audio Settings

□ Mute

Internal microphone input gain:	-10.5 dB
Audio type	○ AAC ● GSM-AMR
AAC bit rate:	128 Kbps
GSM-AMR bit rate:	12.2 Kbps

Mute: Select this option to disable audio transmission from the Network Camera to all clients. Note that if mute mode is turned on, no audio data will be transmitted to all clients even though the audio transmission is enabled on the Client Settings page. In that case, the following message is displayed.



Warning

The media type has been changed to video only because the media from server contains no audio

Internal microphone input gain: There are two options for external microphone input gain, 0db and 20db.

Audio type: Select audio codec AAC or GSM-AMR and the bit rate.

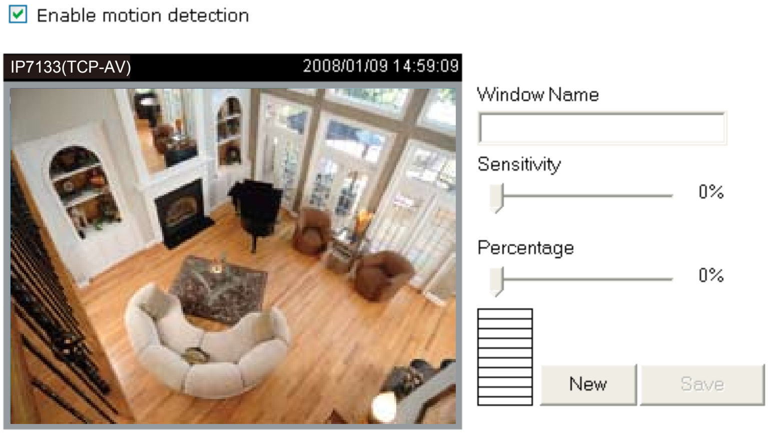
- ■ AAC targets at performing good sound quality at the cost of higher bandwidth consumption. The bit rates are selectable at the following rates: 16Kbps, 32Kbps, 48Kbps, 64Kbps, 96Kbps and128Kbps.

- ■ GSM-ARM is designed to optimize speech quality and requires less bandwidth. The bit rates are selectable at the following rates: 4.75Kbps, 5.15Kbps, 5.90Kbps, 6.7Kbps, 7.4Kbps, 7.95Kbps, 10.2Kbps and 12.2Kbps.

When completed with the settings on this page, click Save to enable the settings.

Motion detection

This section explains how to configure the Network Camera to enable motion detection. A total of three motion detection windows can be configured.



☑ Enable motion detection

IP7133(TCP-AV) 2008/01/09 14:59:09

Window Name

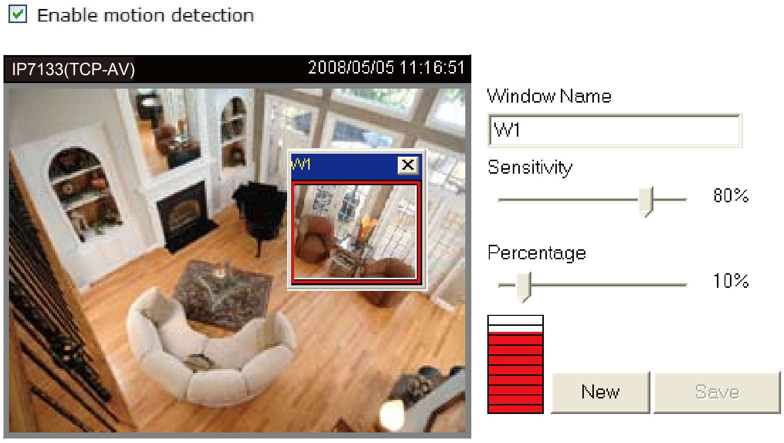
Sensitivity 0%

Percentage 0%

To enable motion detection, follow the steps below:

1. Click **New** to add a new motion detection window.
2. In the Window Name text box, enter a descriptive name for the motion detection window.
   - To move and resize the window, drag-drop the window.
   - To delete window, click X at top right of the window.
3. Define the sensitivity to moving objects and the space ratio of all alerted pixels by moving the Sensitivity and Percentage slider bar.
4. Click **Save** to enable the settings.
5. Select Enable motion detection to enable this function.

For example:



☑ Enable motion detection

IP7133(TCP-AV) 2008/05/05 11:16:51

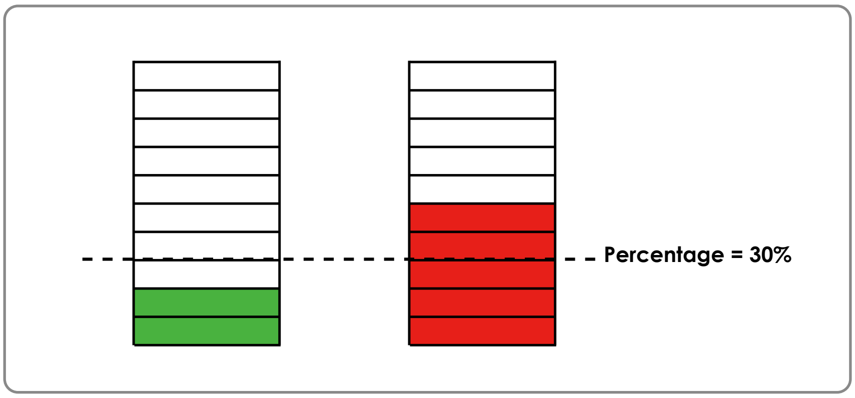
Window Name: W1

Sensitivity 80%

Percentage 10%

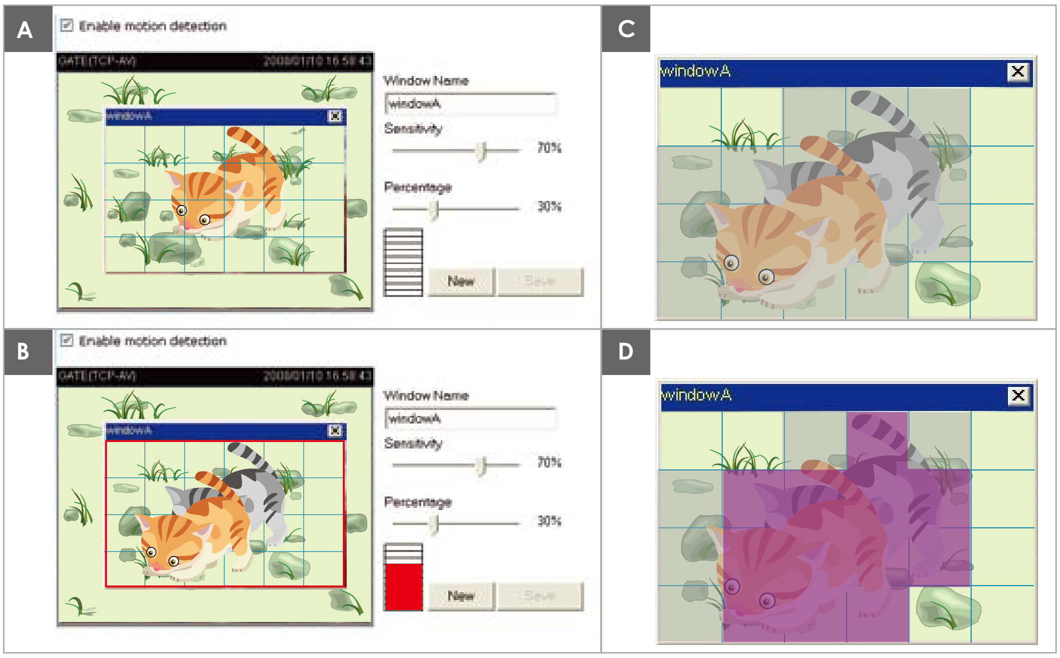
The Percentage Indicator will rise or fall depending on the image variation. When motions are detected by the Network Camera and are judged to exceed the defined threshold, a red bar rises. Meanwhile, the motion detection window will be outlined in red. Photos or videos can be captured instantly and configured to send to the remote server (Email, FTP) by utilizing this feature as a trigger source. For more information on how to plot an event, please refer to Application on page 43.

A green bar indicates that even though motions are detected, the event will not be triggered because the image variations are still falling under the defined threshold.



NOTE

► *How does motion detection work?*



☑ Enable motion detection

Window Name: windowA

Sensitivity: 70%

Percentage: 30%

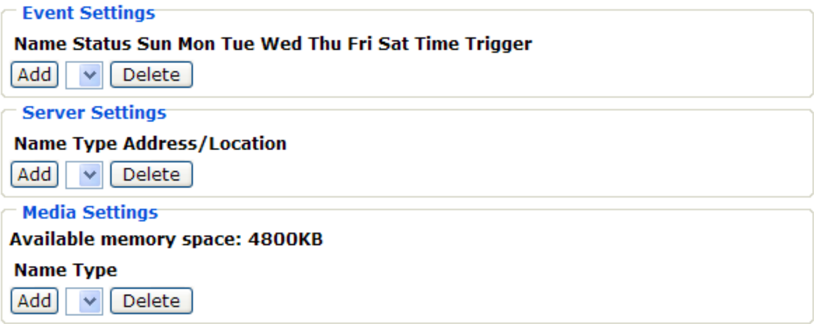
There are two parameters for setting the motion detection: Sensitivity and Percentage. In the illustration above, frame A and frame B are two sequential images. Pixel differences between the two frames are detected and highlighted in gray (frame C), and will be compared with the sensitivity setting. Sensitivity is a value that expresses the sensitivity to moving objects. Higher sensitivity settings are expected to sense a slight movement while smaller sensitivity settings tend to neglect it. When the sensitivity is set to 70%, the Network Camera defines the pixels in the purple areas as "alerted pixels" (frame D).

Percentage is a value that expresses the proportion of "alerted pixels" to all pixels in the motion detection window. In this case, 50% of pixels are identified as "alerted pixels". When the percentage is set to 30%, the motions are judged to exceed the defined threshold; therefore, the motion window will be outlined in red.

For applications that require higher security management, it is suggested to set higher sensitivity settings and smaller percentage values.

Application

This section explains how to configure the Network Camera to react in response to particular situations. A typical application is that when a motion is detected, the Network Camera sends buffered images to a FTP server or via e-mail as notifications.



Event Settings

Name Status Sun Mon Tue Wed Thu Fri Sat Time Trigger

Server Settings

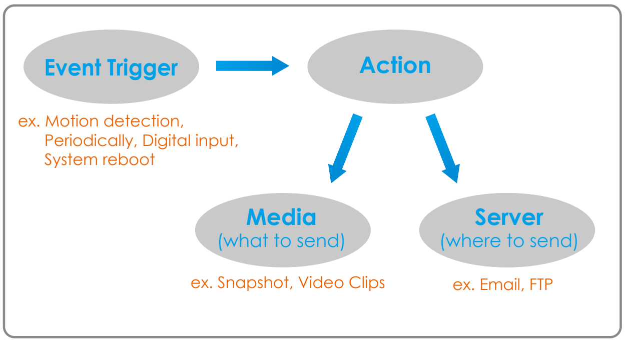
Name Type Address/Location

Media Settings

Available memory space: 4800KB

Name Type

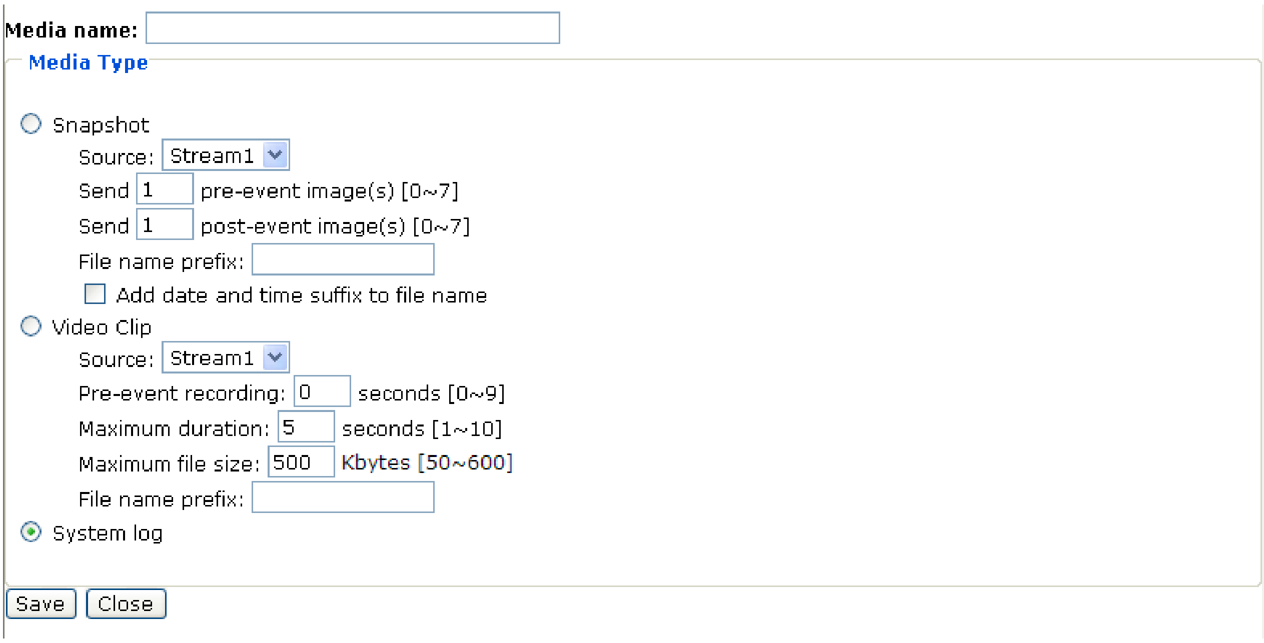
In the illustration on the right side, an event can be triggered by many sources, such as motion detection or external digital input devices. When an event is triggered, you can specify what kind of action will be performed. You can configure the Network Camera to send snapshots or videos to your email address or FTP site.


Event Trigger
Action
ex. Motion detection, Periodically, Digital input, System reboot
Media (what to send)
Server (where to send)
ex. Snapshot, Video Clips
ex. Email, FTP

To start plotting an event, it is suggested to configure server and media columns first so that the Network Camera will know what action shall be performed when a trigger is activated.

Media Settings

In Media Settings column, click **Add** to open the media setting page. On this page, you can specify what kind of media to send when a trigger is activated. A total of five media settings can be configured.



Media name:

Media Type

○ Snapshot

Source: Stream1

Send 1 pre-event image(s) [0~7]

Send 1 post-event image(s) [0~7]

File name prefix:

□ Add date and time suffix to file name

○ Video Clip

Source: Stream1

Pre-event recording: 0 seconds [0~9]

Maximum duration: 5 seconds [1~10]

Maximum file size: 500 Kbytes [50~600]

File name prefix:

● System log

Media name: Enter a descriptive name for the media setting.

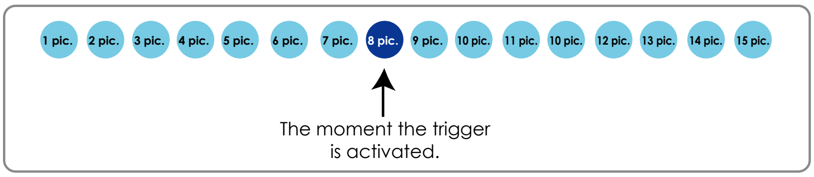
Media Type: There are three choices of media types available: Snapshot, Video Clip, and System log.

Snapshot: Select to send snapshots when a trigger is activated.

■ Source: Select to take snapshots from stream 1 or stream 2.

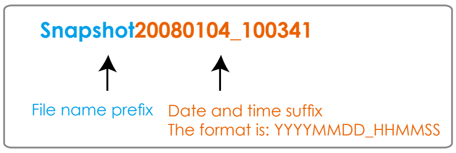
■ Send □ pre-event images
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Specify to capture how many images before a trigger is activated. Up to seven images can be generated.

■ Send □ post-event images
Specify to capture how many images after a trigger is activated. Up to seven images can be generated. For example, if both the Send pre-event images and Send post-event images are set to seven, a total of fifteen images are generated after a trigger is activated.

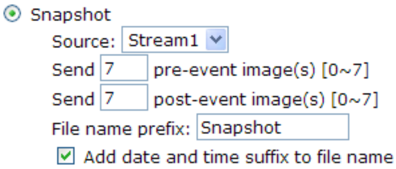


■ File Name Prefix
Enter the text that will be put in front of the file name.

■ Add date and time suffix to the file name
Select this option to add date and time to the file name suffix.



For example:



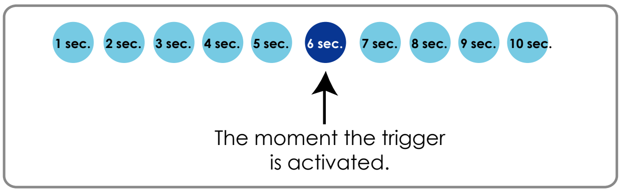
● Snapshot
Source: Stream1
Send 7 pre-event image(s) [0~7]
Send 7 post-event image(s) [0~7]
File name prefix: Snapshot
☑ Add date and time suffix to file name

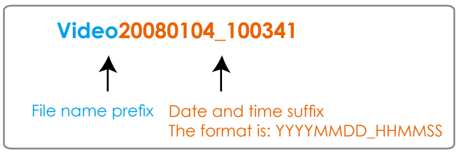
Video Clip: Select to send video clips when a trigger is activated.

■ Source: Select to record video clips from stream 1 or stream 2.

■ Pre-event recording
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Specify to record video clips for how many seconds before a trigger is activated. Up to nine seconds can be set.

■ Maximum duration
Specify the maximal recording duration in seconds. Up to ten seconds can be set.
For example, if the Pre-event recording is set to five seconds and the Maximum duration is set to ten seconds, the Network Camera continues to record for another four seconds after a trigger is activated.

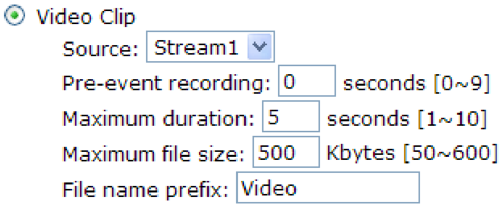




- Maximum file size
  Specify the maximal file size allowed.

- File Name Prefix
  Enter the text that will be put in front of the file name.

For example:



● Video Clip

Source: Stream1

Pre-event recording: 0 seconds [0~9]

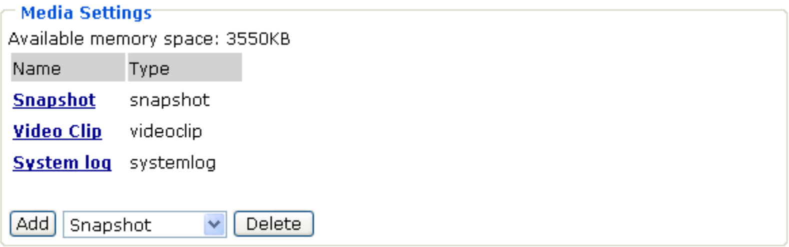
Maximum duration: 5 seconds [1~10]

Maximum file size: 500 Kbytes [50~600]

File name prefix: Video

System log: Select to send a system log when a trigger is activated.

When completed, click **Save** to enable the settings and then click **Close** to exit this page. The new media name will appear in the media drop-down list on the Application page as below. To remove a media setting from the list, select a media name from the drop-down list and then click **Delete**. Note that only when the media setting is not being applied to an event setting can it be deleted.



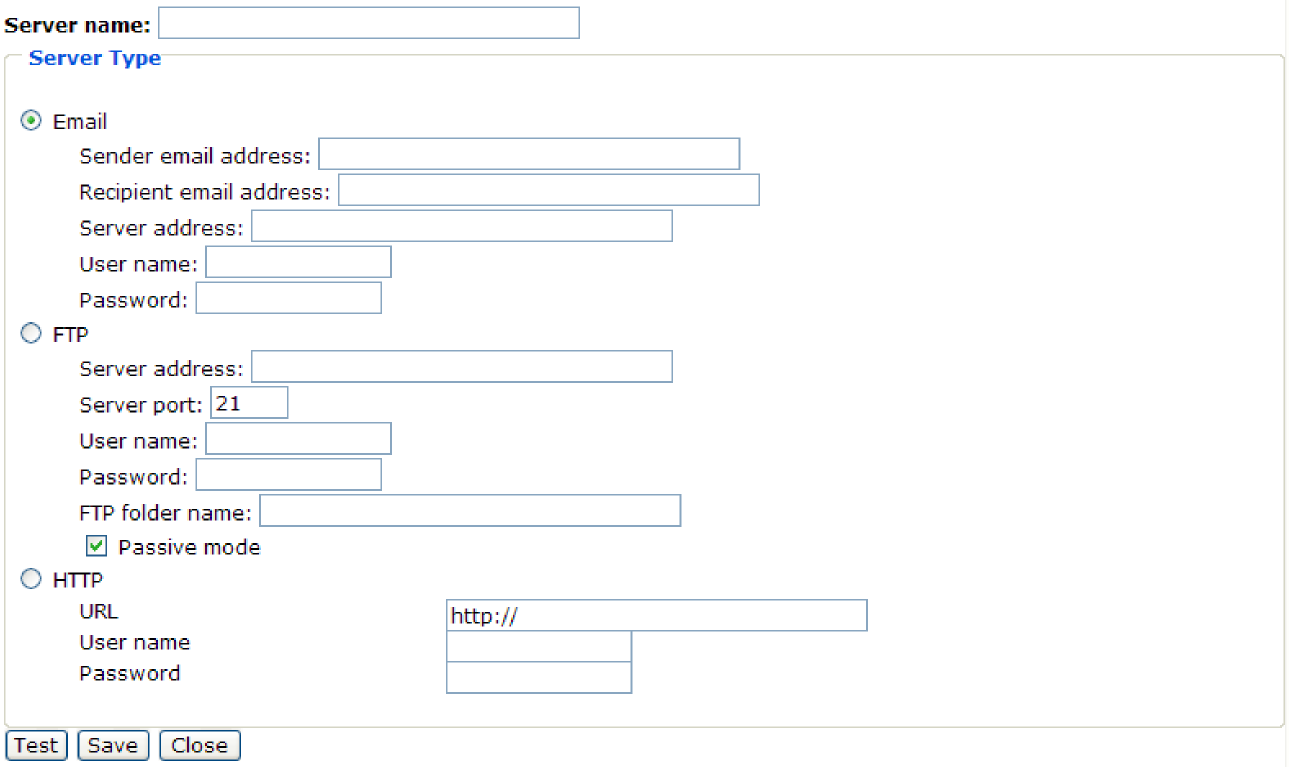
Media Settings

Available memory space: 3550KB

Name	Type
Snapshot	snapshot
Video Clip	videoclip
System log	systemlog

Server Settings

In the Server column, click **Add** to open the server setting page. On this page, you can specify where the notification messages will be send when a trigger is activated. A total of five server settings can be configured.



Server name:

Server Type

● Email

Sender email address:

Recipient email address:

Server address:

User name:

Password:

○ FTP

Server address:

Server port: 21

User name:

Password:

FTP folder name:

☑ Passive mode

○ HTTP

URL http://

User name

Password

Server name: Enter a descriptive name for the server setting.

Server Type: There are four choices of server types available: Email, FTP, and HTTP.

Email: Select to send the media via Email when a trigger is activated.

■ Sender email address: Enter the email address of the sender.

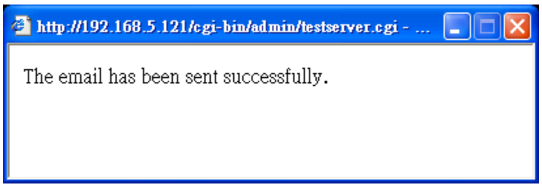
■ Recipient email address: Enter the email address of the recipient.

■ Server address: Enter the domain name or IP address of the email server.

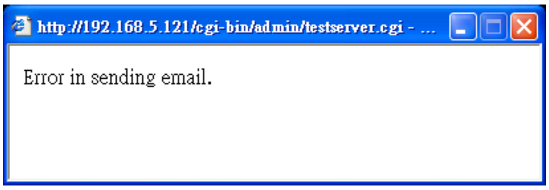
■ User name: Enter the user name of the email account.

■ Password: Enter the password of the email account.

To verify if the email settings are correctly configured, click **Test**. The result will be shown in a pop-up window. If it works, you will also receive an email indicating the result.


http://192.168.5.121/cgi-bin/admin/testserver.cgi - ...

The email has been sent successfully.


http://192.168.5.121/cgi-bin/admin/testserver.cgi - ...

Error in sending email.

FTP: Select to send the media to a FTP server when a trigger is activated.

■ Server address: Enter the domain name or IP address of the FTP server.

■ Server port
By default, the FTP port server is set to 21. Also, it can be assigned with another port number between 1025 and 65535.

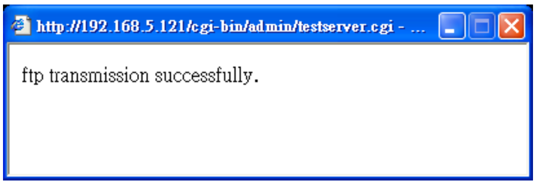
■ User name: Enter the login name of the FTP account.

■ Password: Enter the password of the FTP account.

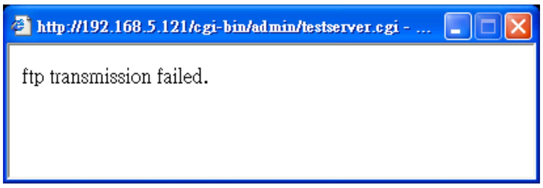
■ FTP folder name
Enter a folder to place the media file. If the folder name does not exist, the Network Camera will create one on the FTP server.

■ Passive mode
Most firewalls do not accept new connections initiated from external requests. If the FTP server supports passive mode, select this option to enable passive mode FTP and allow data transmission to pass through the firewall.

To verify if the FTP settings are correctly configured, click **Test**. The result will be shown in a pop-up window. If it works, you will also receive a test.txt file on the FTP server.


http://192.168.5.121/cgi-bin/admin/testserver.cgi - ...

ftp transmission successfully.


http://192.168.5.121/cgi-bin/admin/testserver.cgi - ...

ftp transmission failed.

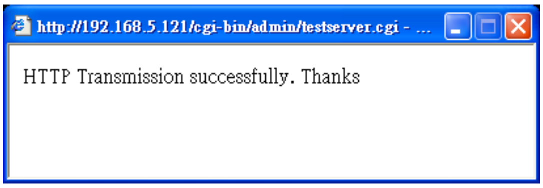
HTTP: Select to send the media to a HTTP server when a trigger is activated.

■ URL: Enter the URL of the HTTP server.

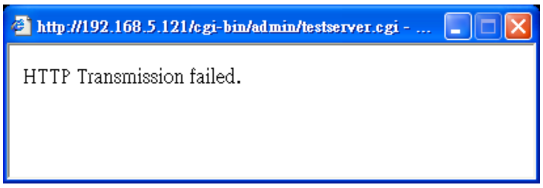
■ User name: Enter the user name.

■ Password: Enter the password.

To verify if the HTTP settings are correctly configured, click **Test**. The result will be shown in a pop-up window. If it works, you will also receive a test.txt file on the HTTP server.

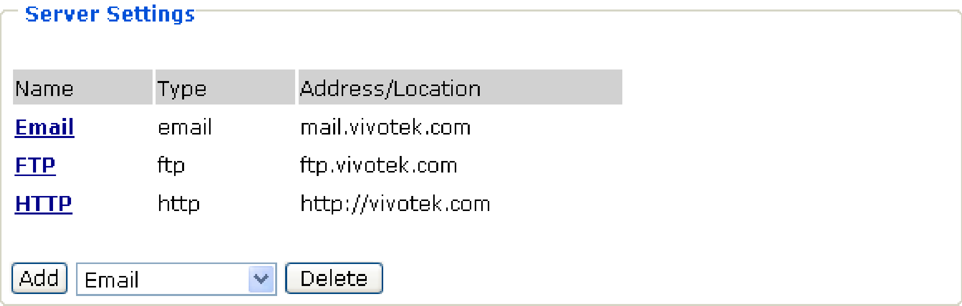


HTTP Transmission successfully. Thanks



HTTP Transmission failed.

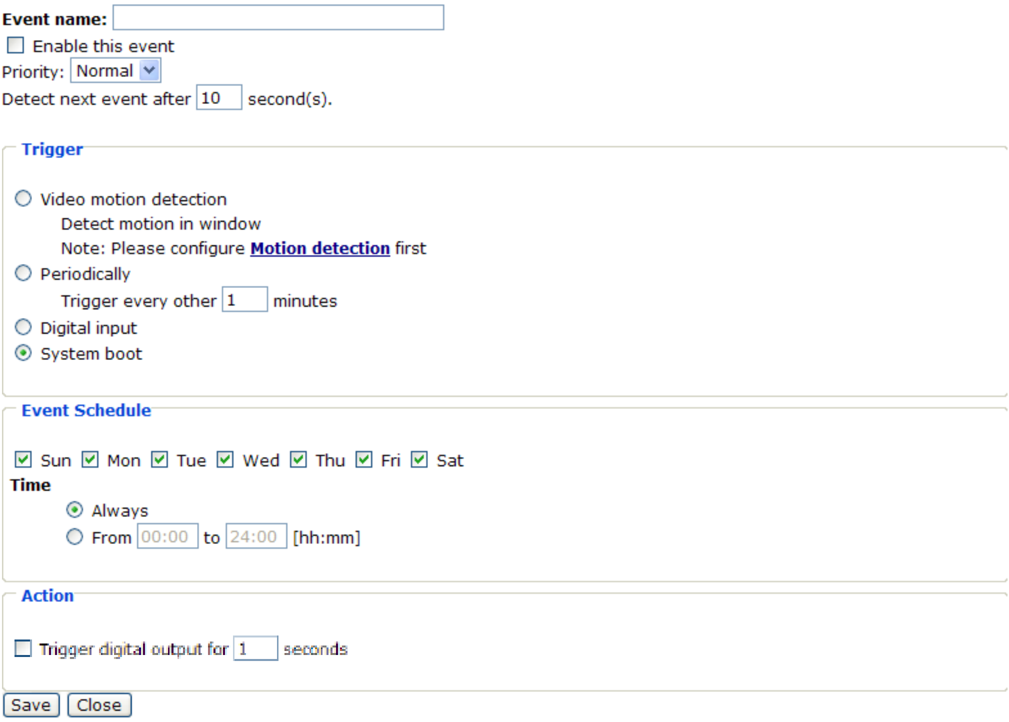
When completed, click **Save** to enable the settings and then click **Close** to exit this page. The new server name will appear in the server drop-down list on the application page as below. To remove a server setting from the list, select a server name from the drop-down list and then click Delete. Note that only when the server setting is not being applied to an event setting can it be deleted.



Name	Type	Address/Location
Email	email	mail.vivotek.com
FTP	ftp	ftp.vivotek.com
HTTP	http	http://vivotek.com

Event Settings

In the Event column, click Add to open the event setting page. On this page, you can arrange the three elements -- Trigger, Schedule and Action to plot an event. A total of three event settings can be configured.



Event name:

□ Enable this event

Priority: Normal

Detect next event after 10 second(s).

Trigger

○ Video motion detection
Detect motion in window
Note: Please configure **Motion detection** first

○ Periodically
Trigger every other 1 minutes

○ Digital input

● System boot

Event Schedule

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time

● Always

○ From 00:00 to 24:00 [hh:mm]

Action

□ Trigger digital output for 1 seconds

Event name: Enter a descriptive name for the event setting.

Enable this event: Select this option to enable this event setting.

Priority: Select the relative importance of this event (High, Normal, and Low). Events with higher priority setting will be executed first.

Detect next event after □ seconds: Enter the duration in seconds to pause motion detection after a motion is detected.

An event is an action initiated by user-defined trigger source; it is the causal arrangement of the following three elements: Trigger, Event Schedule, and Action.

Trigger: Also referred as the cause or stimulus, defines when to trigger the Network Camera. The trigger source can be configured to use the Network Camera's built-in motion detection mechanism or external digital input devices.There are four choices of trigger sources:

■ Video motion detection
Select this option to allow the Network Camera to use the built-in motion detection mechanism as a trigger source. To enable this function, you need to configure Motion detection first. For more information, please refer to Motion detection on page 41 for details.

■ Periodically
Select this option to allow the Network Camera to trigger periodically for every other defined minute. At most 999 minutes can be set.

■ Digital input
Select one of the Digital inputs to allow the Network Camera to use external digital input device as a trigger source. Depending on your applications, there are choices of digital input devices on the market which helps to sense any changes in temperature, vibration, sound and light, etc.

- System boot
  Select this option to allow the Network Camera to trigger when the power of Network Camera is disconnected.

Event Schedule: The effective period in which the event stays active. Specify the effective period for the event.

- Select the days on weekly basis.

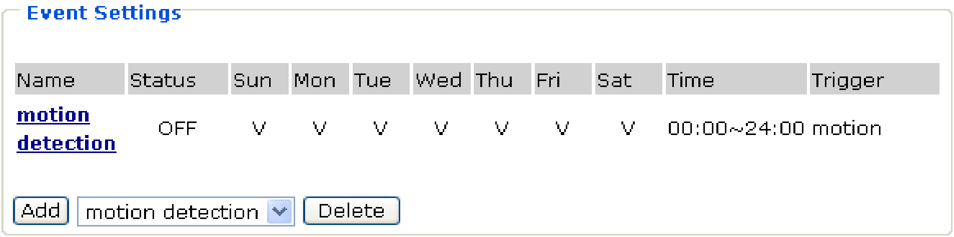
- Select the time for recording in 24-hr time format.

Action: Also referred as the effect, defines the action to be performed by the Network Camera when the trigger is activated. Select the action to perfom when a trigger is activated.

- Trigger digital output for □ seconds
  Select this option to turn on external digital output device when a trigger is activated. Specify the length of trigger interval in the text box.

- Server name / Media name
  Select the server and media name to allow the Network Camera to send the media files to the server when a trigger is activated.

When completed, select Enable this event. Click **Save** to enable the settings and then click **Close** to exit this page. The new event name will appear in the event drop-down list on the application page. To remove an event setting from the list, select an event name from the drop-down list and then click **Delete**.



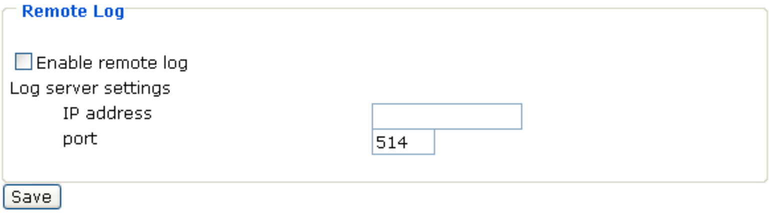
Event Settings

Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Trigger
motion detection	OFF	V	V	V	V	V	V	V	00:00~24:00	motion

System log

This section explains how to configure the Network Camera to send system log to remote server as a backup. It is composed of the following two columns: Remote Log and Current Log.

Remote Log



Remote Log

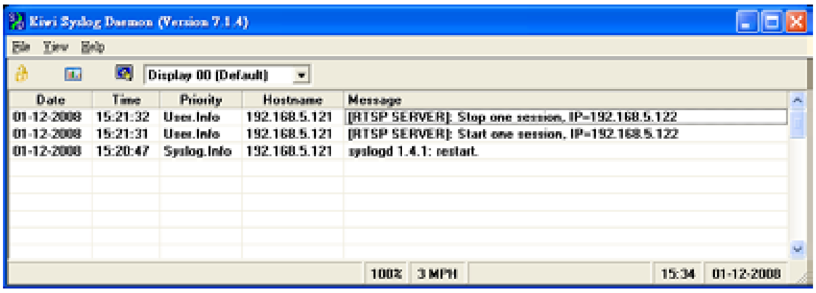
☐ Enable remote log

Log server settings

IP address

port 514

You can configure the Network Camera to send the system log file to a remote server as a log backup. Before utilizing this feature, it is suggested to install a log-recording tool to receive system log messages from the Network Camera. For example, a tool -- Kiwi Syslog Daemon. Visit http://www.kiwisyslog.com/kiwi-syslog-daemon-overview/.

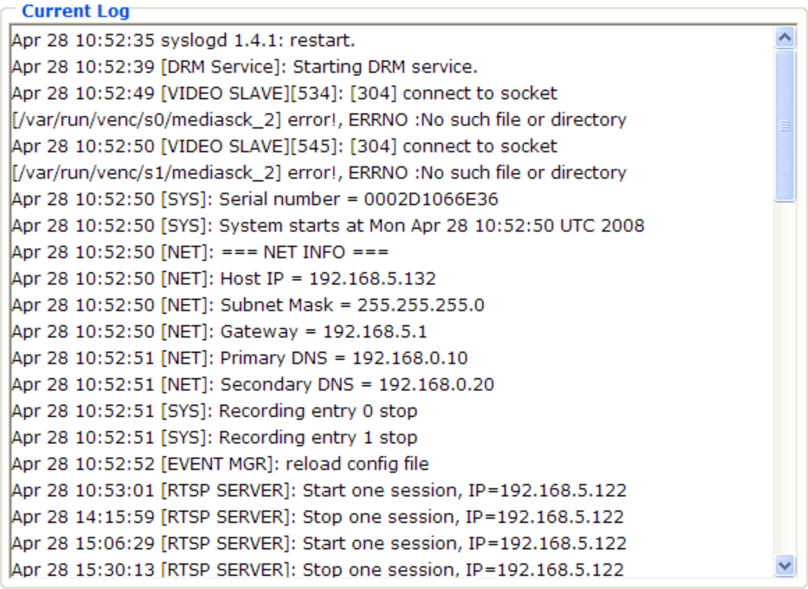


Date	Time	Priority	Hostname	Message
01-12-2008	15:21:32	User.Info	192.168.5.121	[RTSP SERVER]: Stop one session, IP=192.168.5.122
01-12-2008	15:21:31	User.Info	192.168.5.121	[RTSP SERVER]: Start one session, IP=192.168.5.122
01-12-2008	15:20:47	Syslog.Info	192.168.5.121	syslogd 1.4.1: restart.

Follow the steps below to set up the remote log:

1. In the IP address text box, enter the IP address of the remote server.
2. In the port text box, enter the port number of the remote server.
3. When completed, select Enable remote log and click Save to enable the settings.

Current Log



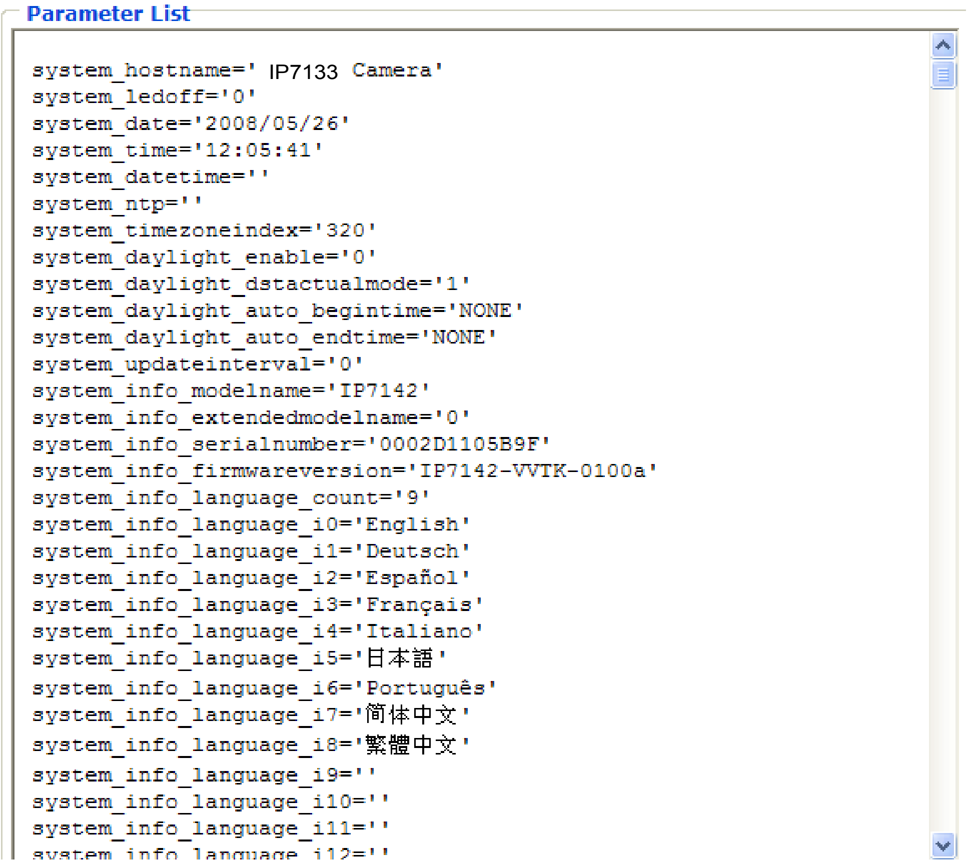
Current Log

```
Apr 28 10:52:35 syslogd 1.4.1: restart.
Apr 28 10:52:39 [DRM Service]: Starting DRM service.
Apr 28 10:52:49 [VIDEO SLAVE][534]: [304] connect to socket
[/var/run/venc/s0/mediasck_2] error!, ERRNO :No such file or directory
Apr 28 10:52:50 [VIDEO SLAVE][545]: [304] connect to socket
[/var/run/venc/s1/mediasck_2] error!, ERRNO :No such file or directory
Apr 28 10:52:50 [SYS]: Serial number = 0002D1066E36
Apr 28 10:52:50 [SYS]: System starts at Mon Apr 28 10:52:50 UTC 2008
Apr 28 10:52:50 [NET]: === NET INFO ===
Apr 28 10:52:50 [NET]: Host IP = 192.168.5.132
Apr 28 10:52:50 [NET]: Subnet Mask = 255.255.255.0
Apr 28 10:52:50 [NET]: Gateway = 192.168.5.1
Apr 28 10:52:51 [NET]: Primary DNS = 192.168.0.10
Apr 28 10:52:51 [NET]: Secondary DNS = 192.168.0.20
Apr 28 10:52:51 [SYS]: Recording entry 0 stop
Apr 28 10:52:51 [SYS]: Recording entry 1 stop
Apr 28 10:52:52 [EVENT MGR]: reload config file
Apr 28 10:53:01 [RTSP SERVER]: Start one session, IP=192.168.5.122
Apr 28 14:15:59 [RTSP SERVER]: Stop one session, IP=192.168.5.122
Apr 28 15:06:29 [RTSP SERVER]: Start one session, IP=192.168.5.122
Apr 28 15:30:13 [RTSP SERVER]: Stop one session, IP=192.168.5.122
```

This column displays the system's log in chronological order. The system log is stored in the Network Camera's buffer area and will be overwritten when reaching a certain amount.

View parameters

The View parameters page lists the entire system's parameters in alphabetical order. If you need technical assistance, please provide the information listed On this page.

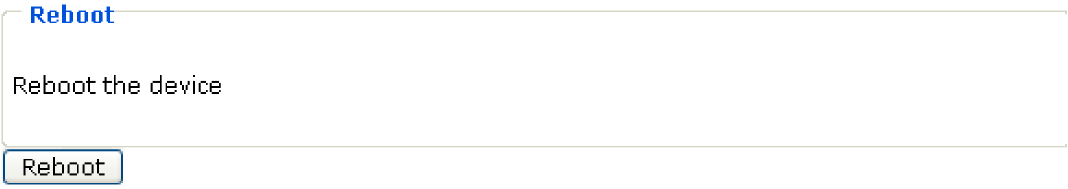


```
system_hostname=' IP7133 Camera'
system_ledoff='0'
system_date='2008/05/26'
system_time='12:05:41'
system_datetime=''
system_ntp=''
system_timezoneindex='320'
system_daylight_enable='0'
system_daylight_dstactualmode='1'
system_daylight_auto_begintime='NONE'
system_daylight_auto_endtime='NONE'
system_updateinterval='0'
system_info_modelname='IP7142'
system_info_extendedmodelname='0'
system_info_serialnumber='0002D1105B9F'
system_info_firmwareversion='IP7142-VVTK-0100a'
system_info_language_count='9'
system_info_language_i0='English'
system_info_language_i1='Deutsch'
system_info_language_i2='Español'
system_info_language_i3='Français'
system_info_language_i4='Italiano'
system_info_language_i5='日本語'
system_info_language_i6='Português'
system_info_language_i7='简体中文'
system_info_language_i8='繁體中文'
system_info_language_i9=''
system_info_language_i10=''
system_info_language_i11=''
system_info_language_i12=''
```

Maintenance

This chapter explains how to restore the Network Camera to factory default, upgrade firmware version, etc.

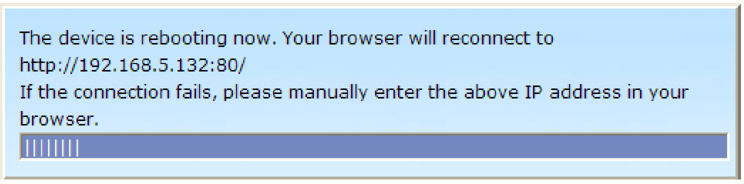
Reboot



Reboot

Reboot the device

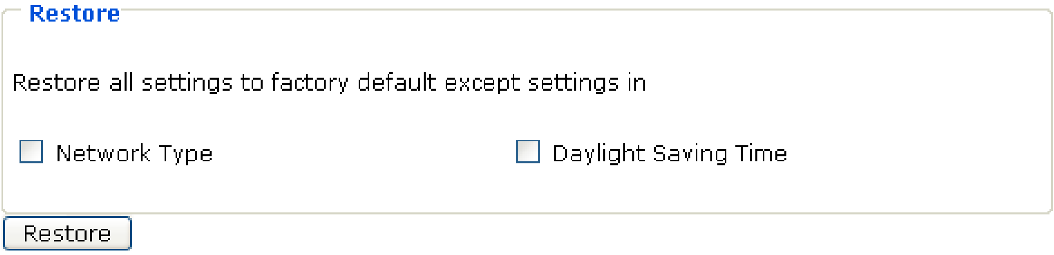
This feature allows you to turn off and then turn on the Network Camera. It takes about one ~ two minutes to complete the process. When completed, the live video will be displayed in your browser. The following message is displayed during the rebooting process.



The device is rebooting now. Your browser will reconnect to
http://192.168.5.132:80/
If the connection fails, please manually enter the above IP address in your browser.

If the connection fails after rebooting, manually enter the IP address of the Network Camera in the address field to resume the connection.

Restore



Restore

Restore all settings to factory default except settings in

☐ Network Type ☐ Daylight Saving Time

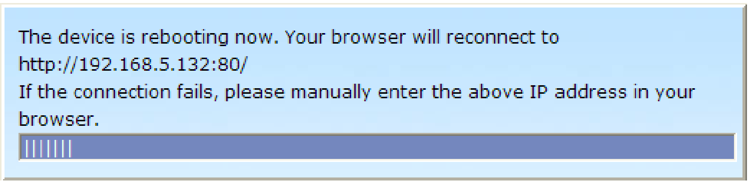
This feature allows you to restore the Network Camera to factory default. Two settings can be excluded:

Network Type: Select this option to retain the Network Type settings (please refer to Network Type on page 23).

Daylight Saving Time: Select this option to retain the Daylight Saving Time settings (please refer to System on page 20)

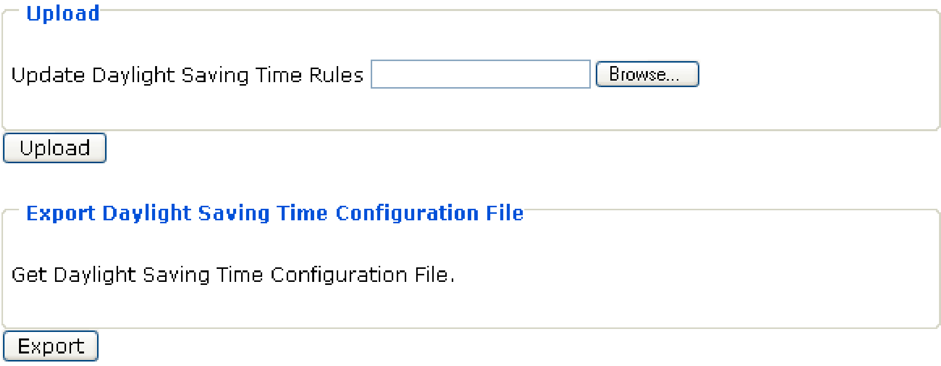
If none of the options is selected, all settings will be restored to factory default.

The following message is displayed during the restoring process.



The device is rebooting now. Your browser will reconnect to
http://192.168.5.132:80/
If the connection fails, please manually enter the above IP address in your browser.

Upload / Export Daylight Saving Time Configuration File



Upload

Update Daylight Saving Time Rules [Browse...]

[Upload]

Export Daylight Saving Time Configuration File

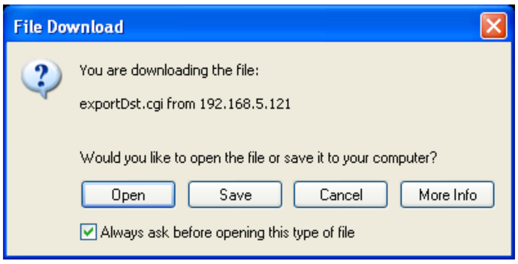
Get Daylight Saving Time Configuration File.

[Export]

This feature allows you to set the starting time and ending time of DST.

Follow the steps below to set up:

1. In the Export Daylight Saving Time Configuration File Column, click Export to export an Extensible Markup Language (*.xml) file from the Network Camera.
2. Open the XML file using Microsoft® Notepad and locate your time zone; set the starting time and ending time of the DST. When completed, save the file.



File Download

You are downloading the file:

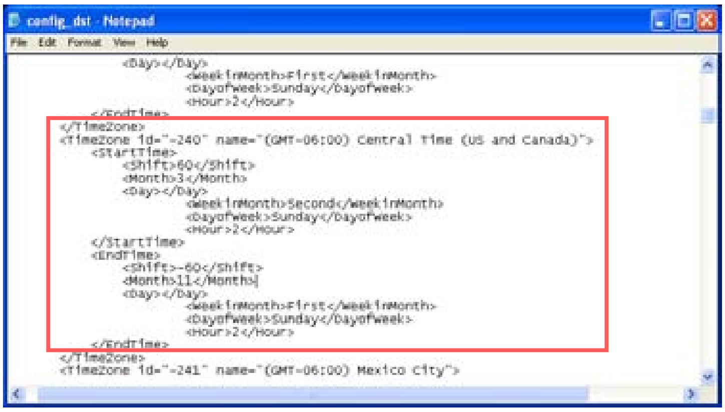
exportDst.cgi from 192.168.5.121

Would you like to open the file or save it to your computer?

[Open] [Save] [Cancel] [More Info]

☑ Always ask before opening this type of file

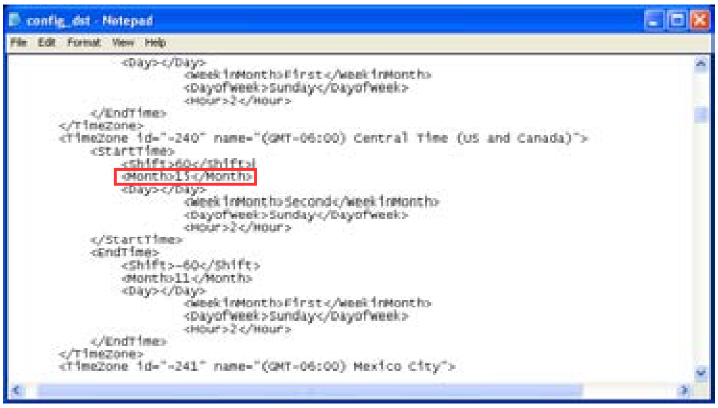
In the example below, the DST begins each year at 2:00 a.m. on the second Sunday in March and ends at 2:00 a.m. on the first Sunday in November.



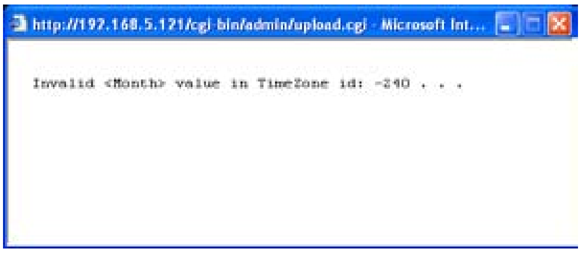
```
            <Day></Day>
                    <WeekInMonth>First</WeekInMonth>
                    <DayofWeek>Sunday</DayofWeek>
                    <Hour>2</Hour>
        </EndTime>
    </TimeZone>
    <TimeZone id="-240" name="(GMT-06:00) Central Time (US and Canada)">
        <StartTime>
            <Shift>60</Shift>
            <Month>3</Month>
            <Day></Day>
                    <WeekInMonth>Second</WeekInMonth>
                    <DayofWeek>Sunday</DayofWeek>
                    <Hour>2</Hour>
        </StartTime>
        <EndTime>
            <Shift>-60</Shift>
            <Month>11</Month>
            <Day></Day>
                    <WeekInMonth>First</WeekInMonth>
                    <DayofWeek>Sunday</DayofWeek>
                    <Hour>2</Hour>
        </EndTime>
    </TimeZone>
    <TimeZone id="-241" name="(GMT-06:00) Mexico City">
```

3. In the Upload Column, click Browse… and specify the XML file.

   If the incorrect date and time is assigned, you will see the following warning message when uploading the file to the Network Camera.

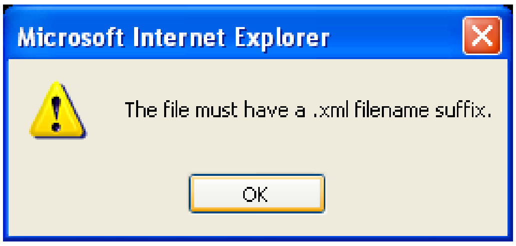


```
            <Day></Day>
                    <WeekInMonth>First</WeekInMonth>
                    <DayofWeek>Sunday</DayofWeek>
                    <Hour>2</Hour>
        </EndTime>
    </TimeZone>
    <TimeZone id="-240" name="(GMT-06:00) Central Time (US and Canada)">
        <StartTime>
            <Shift>60</Shift>
            <Month>15</Month>
            <Day></Day>
                    <WeekInMonth>Second</WeekInMonth>
                    <DayofWeek>Sunday</DayofWeek>
                    <Hour>2</Hour>
        </StartTime>
        <EndTime>
            <Shift>-60</Shift>
            <Month>11</Month>
            <Day></Day>
                    <WeekInMonth>First</WeekInMonth>
                    <DayofWeek>Sunday</DayofWeek>
                    <Hour>2</Hour>
        </EndTime>
    </TimeZone>
    <TimeZone id="-241" name="(GMT-06:00) Mexico City">
```


http://192.168.5.121/cgi-bin/admin/upload.cgi - Microsoft Int...

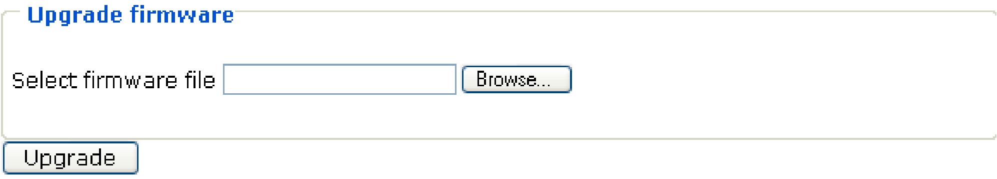
```
Invalid <Month> value in TimeZone id: -240 . . .
```

4. Click Upload. To enable the DST, see System Time on page 22.
   The following message is displayed when attempting to upload an incorrect file format.



The file must have a .xml filename suffix.

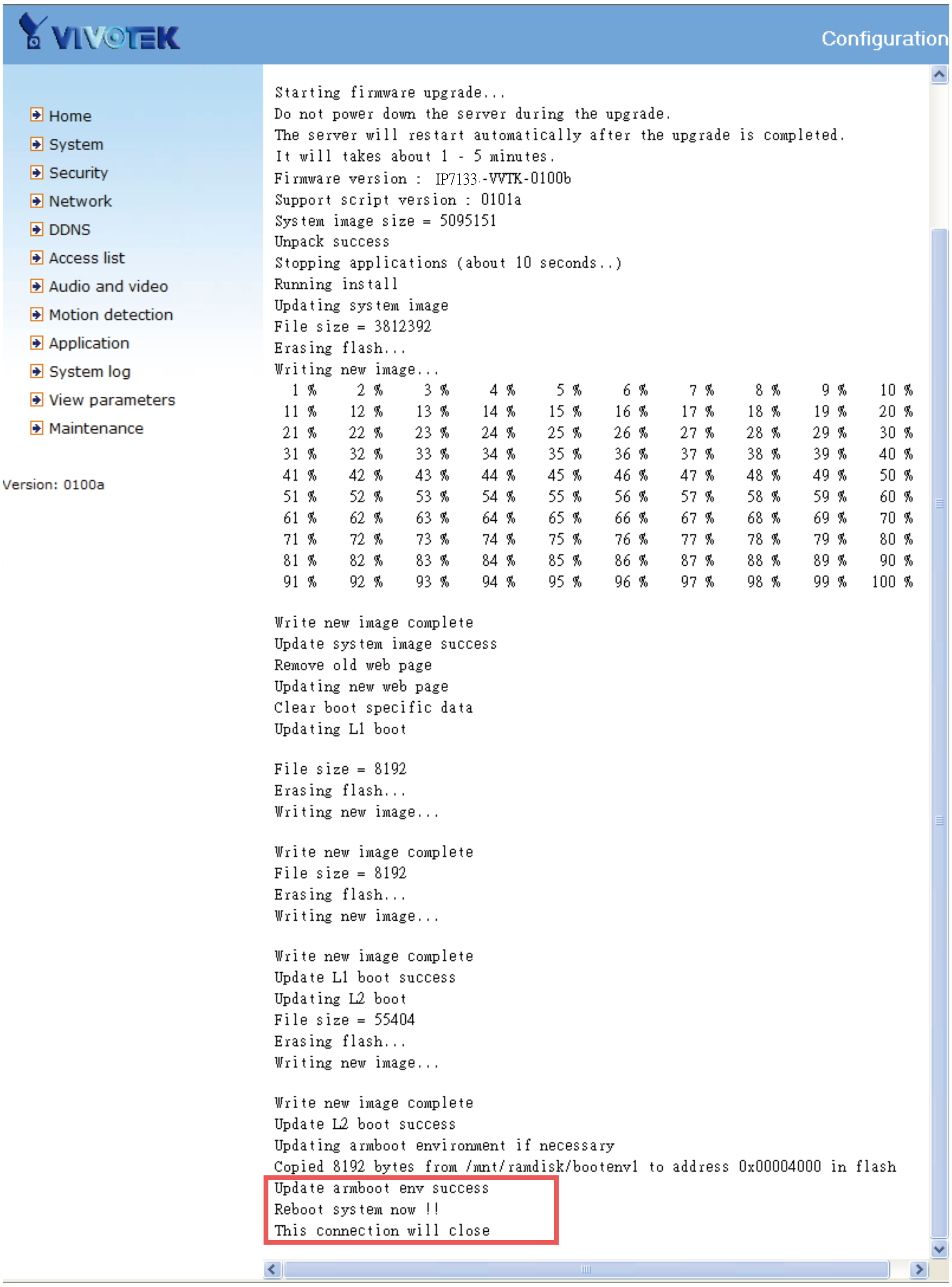
Upgrade Firmware



This feature allows you to upgrade the firmware on your Network Camera. It takes about five minutes to complete the process.
Note that do not power off the Network Camera during the upgrade.

Follow the steps below to upgrade firmware:
1. Download a new firmware file from VIVOTEK website. The file is in pkg file format.
2. Click Browse… and specify the firmware file.
3. Click Upgrade. The Network Camera starts to upgrade and will reboot automatically when the upgrade completes.

The upgrade is successful as you see “Reboot system now!! This connection will close”. After that, re-access the Network Camera.
The following message is displayed when the upgrade is succeeded.



```
Starting firmware upgrade...
Do not power down the server during the upgrade.
The server will restart automatically after the upgrade is completed.
It will takes about 1 - 5 minutes.
Firmware version :  IP7133-VVTK-0100b
Support script version : 0101a
System image size = 5095151
Unpack success
Stopping applications (about 10 seconds..)
Running install
Updating system image
File size = 3812392
Erasing flash...
Writing new image...
  1 %     2 %     3 %     4 %     5 %     6 %     7 %     8 %     9 %    10 %
 11 %    12 %    13 %    14 %    15 %    16 %    17 %    18 %    19 %    20 %
 21 %    22 %    23 %    24 %    25 %    26 %    27 %    28 %    29 %    30 %
 31 %    32 %    33 %    34 %    35 %    36 %    37 %    38 %    39 %    40 %
 41 %    42 %    43 %    44 %    45 %    46 %    47 %    48 %    49 %    50 %
 51 %    52 %    53 %    54 %    55 %    56 %    57 %    58 %    59 %    60 %
 61 %    62 %    63 %    64 %    65 %    66 %    67 %    68 %    69 %    70 %
 71 %    72 %    73 %    74 %    75 %    76 %    77 %    78 %    79 %    80 %
 81 %    82 %    83 %    84 %    85 %    86 %    87 %    88 %    89 %    90 %
 91 %    92 %    93 %    94 %    95 %    96 %    97 %    98 %    99 %   100 %

Write new image complete
Update system image success
Remove old web page
Updating new web page
Clear boot specific data
Updating L1 boot

File size = 8192
Erasing flash...
Writing new image...

Write new image complete
File size = 8192
Erasing flash...
Writing new image...

Write new image complete
Update L1 boot success
Updating L2 boot
File size = 55404
Erasing flash...
Writing new image...

Write new image complete
Update L2 boot success
Updating armboot environment if necessary
Copied 8192 bytes from /mnt/ramdisk/bootenv1 to address 0x00004000 in flash
Update armboot env success
Reboot system now !!
This connection will close
```

The following message is displayed when you have selected an incorrect firmware file.

```
Starting firmware upgrade...
Do not power down the server during the upgrade.
The server will restart automatically after the upgrade is
completed.
It will takes about 1 - 5 minutes.
Wrong PKG file format
Unpack fail
```

Appendix

URL Commands of the Network Camera

Overview

For some customers who already have their own web site or web control application, Network Camera/ Video server can be easily integrated through convenient URLs. This section specifies the external HTTP based application programming interface. The HTTP based camera interface provides the functionality to request a single image, to control camera functions and to get and set internal parameter values. The image and CGI-requests are handled by the built in Web server.

Style convention

In URL syntax and in descriptions of CGI parameters, a text within angle brackets denotes a content that is to be replaced with either a value or a string. When replacing the text string also the angle brackets shall be replaced. An example of this is the description of the name for the server, denoted with <servername> in the URL syntax description below, that is replaced with the string myserver in the URL syntax example, also below.

URL syntax' are written with the “**Syntax:**" word written in bold face followed by a box with the referred syntax as seen below. The name of the server is written as <servername>. This is intended to be replaced with the name of the actual server. This can either be a name, e.g., "mywebcam" or "thecam. adomain.net" or the associated IP number for the server, e.g., 192.168.0.220.

Syntax:

```
http://<servername>/cgi-bin/viewer/video.jpg
```

Description of returned data is written with "**Return:**" in bold face followed by the returned data in a box. All data returned as HTTP formatted, i.e., starting with the string HTTP is line separated with a Carriage Return and Line Feed (CRLF) printed as \r\n.

Return:

```
HTTP/1.0 <HTTP code> <HTTP text>\r\n
```

URL syntax examples are written with "**Example:**" in bold face followed by a short description and a light grey box with the example.

Example: request a single snapshot image

```
http://mywebserver/cgi-bin/viewer/video.jpg
```

General CGI URL Syntax and Parameters

CGI parameters are written in lower-case and as one word without any underscores or other separators. When the CGI request includes internal camera parameters, these parameters must be written exactly as they are named in the camera or video server. The CGIs are organized in functionally-related directories under the cgi-bin directory. The file extension .cgi is required.

Syntax:

```
http://<servername>/cgi-bin/<subdir>[/<subdir>...]/<cgi>.<ext>
[?<parameter>=<value>[&<parameter>=<value>...]]
```

Example: Set digital output #1 to active

```
http://mywebserver/cgi-bin/dido/setdo.cgi?do1=1
```

Security Level

SECURITY LEVEL	SUB-DIRECTORY	DESCRIPTION
0	anonymous	Unprotected.
1 [view]	anonymous, viewer, dido, camctrl	1. Can view, listen, talk to camera. 2. Can control DI/DO, PTZ of the camera.
4 [operator]	anonymous, viewer, dido, camctrl, operator	Operator access rights can modify most of the camera's parameters except some privileges and network options.
6 [admin]	anonymous, viewer, dido, camctrl, operator, admin	Administrator access rights can fully control the camera's operations.
7	N/A	Internal parameters. Unable to be changed by any external interfaces.

Get Server Parameter Values

Note: The access right depends on the URL directory.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/anonymous/getparam.cgi?[<parameter>]
[&<parameter>…]

http://<servername>/cgi-bin/viewer/getparam.cgi?[<parameter>]
```

```
[&<parameter>…]

http://<servername>/cgi-bin/operator/getparam.cgi?[<parameter>]
[&<parameter>…]

http://<servername>/cgi-bin/admin/getparam.cgi?[<parameter>]
[&<parameter>…]
```

Where the *<parameter>* should be *<group>*[_*<name>*] or *<group>*[.*<name>*]. If you do not specify any parameters, all the parameters on the server will be returned. If you specify only *<group>*, the parameters of the related group will be returned.

When querying parameter values, the current parameter values are returned.

A successful control request returns parameter pairs as follows:

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: <length>\r\n
\r\n
<parameter pair>
```

where <parameter pair> is

<parameter>=<value>\r\n

[<parameter pair>]

<length> is the actual length of content.

Example: Request IP address and its response

```
Request:
http://192.168.0.123/cgi-bin/admin/getparam.cgi?network_ipaddress

Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: 33\r\n
\r\n
network.ipaddress=192.168.0.123\r\n
```

Set Server Parameter Values

Note: The access right depends on the URL directory.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/anonymous/setparam.cgi? <parameter>=<value>
[&<parameter>=<value>…][&update=<value>][&return=<return page>]

http://<servername>/cgi-bin/viewer/setparam.cgi? <parameter>=<value>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]

http://<servername>/cgi-bin/operator/setparam.cgi? <parameter>=<value>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]

http://<servername>/cgi-bin/admin/setparam.cgi? <parameter>=<value>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
<group>_<name>	value to assigned	Assign *<value>* to the parameter *<group>_<name>.*
update	<boolean>	Set to 1 to update all fields (no need to update parameter in each group).
return	*<return page>*	Redirect to the page *<return page>* after the parameter is assigned*.* The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page. (Note: The return page can be a general HTML file (.htm, .html) or a VIVOTEK server script executable (.vspx) file. It cannot be a CGI command or have any extra parameters. This parameter must be placed at the end of the parameter list

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: <length>\r\n
\r\n
<parameter pair>
```

where <parameter pair> is

<parameter>=<value>\r\n

[<parameter pair>]

Only the parameters that you set and are readable will be returned.

Example: Set the IP address of server to 192.168.0.123:

```
Request:
http://myserver/cgi-bin/admin/setparam.cgi?network_ipaddress=192.168.0.123

Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: 33\r\n
\r\n
network.ipaddress=192.168.0.123\r\n
```

Available parameters on the server

Valid values:

VALID VALUES	DESCRIPTION
string[<n>]	Text strings shorter than ‘n’ characters. The characters “,’, <,>,& are invalid.
string[n~m]	Text strings longer than `n’ characters and shorter than `m’ characters. The characters “,’, <,>,& are invalid.
password[<n>]	The same as string but displays ‘*’ instead.
integer	Any number between (-2^{31} – 1) and (2^{31} – 1).
positive integer	Any number between 0 and (2^{32} – 1).
<m> ~ <n>	Any number between ‘m’ and ‘n’.
domain name[<n>]	A string limited to a domain name shorter than ‘n’ characters (eg. www.ibm.com).
email address [<n>]	A string limited to an email address shorter than ‘n’ characters (eg. joe@www.ibm.com).
ip address	A string limited to an IP address (eg. 192.168.1.1).
mac address	A string limited to contain a MAC address without hyphens or colons.
boolean	A boolean value of 1 or 0 represents [Yes or No], [True or False], [Enable or Disable].
<value1>, <value2>, <value3>, …	Enumeration. Only given values are valid.

blank	A blank string.
everything inside <>	A description
positive Integer	Any number between 0 and (2^{32} – 1)
integer primary key	SQLite data type. A 32-bit signed integer. The value is assigned a unique integer by the server.
text	SQLite data type. The value is a text string, stored using the database encoding (UTF-8, UTF-16BE or UTF-16-LE).
coordinate	x, y coordinate (eg. 0,0)
window size	window width and height (eg. 800x600)

NOTE: The camera should not be restarted when parameters are changed.

Group: **system**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
hostname	string[40]	1/6	Host name of server (Network Camera, Wireless Network Camera, Video Server, Wireless Video Server).
ledoff	<boolean>	6/6	Turn on (0) or turn off (1) all led indicators.
date	<yyyy/mm/dd>, keep, auto	6/6	Current date of system. Set to ‘keep’ to keep date unchanged. Set to ‘auto’ to use NTP to synchronize date.
time	<hh:mm:ss>, keep, auto	6/6	Current time of the system. Set to ‘keep’ to keep time unchanged. Set to ‘auto’ to use NTP to synchronize time.
datetime	<MMDDhhmmYYYY.ss>	6/6	Another current time format of the system.
ntp	<domain name>, <ip address>, <blank>	6/6	NTP server. *Do not use “skip to invoke default server” for default value.
timezoneindex	-489 ~ 529	6/6	Indicate timezone and area. -480: GMT-12:00 Eniwetok, Kwajalein -440: GMT-11:00 Midway Island, Samoa -400: GMT-10:00 Hawaii -360: GMT-09:00 Alaska -320: GMT-08:00 Las Vegas, San_Francisco, Vancouver -280: GMT-07:00 Mountain Time, Denver

			-281: GMT-07:00 Arizona -240: GMT-06:00 Central America, Central Time, Mexico City, Saskatchewan -200: GMT-05:00 Eastern Time, New York, Toronto -201: GMT-05:00 Bogota, Lima, Quito, Indiana -160: GMT-04:00 Atlantic Time, Caracas, Canada, La Paz, Santiago -140: GMT-03:30 Newfoundland -120: GMT-03:00 Brasilia, Buenos Aires, Georgetown, Greenland -80: GMT-02:00 Mid-Atlantic -40: GMT-01:00 Azores, Cape_Verde_IS. 0: GMT Casablanca, Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London 40: GMT 01:00 Amsterdam, Berlin, Rome, Stockholm, Vienna, Madrid, Paris 41: GMT 01:00 Warsaw, Budapest, Bern 80: GMT 02:00 Athens, Helsinki, Istanbul, Riga 81: GMT 02:00 Cairo 82: GMT 02:00 Lebanon, Minsk 83: GMT 02:00 Israel 120: GMT 03:00 Baghdad, Kuwait, Riyadh, Moscow, St. Petersburg, Nairobi 121: GMT 03:00 Iraq 140: GMT 03:30 Tehran 160: GMT 04:00 Abu Dhabi, Muscat, Baku, Tbilisi, Yerevan 180: GMT 04:30 Kabul 200: GMT 05:00 Ekaterinburg, Islamabad, Karachi, Tashkent 220: GMT 05:30 Calcutta, Chennai, Mumbai, New Delhi 230: GMT 05:45 Kathmandu 240: GMT 06:00 Almaty, Novosibirsk, Astana, Dhaka, Sri Jayawardenepura 260: GMT 06:30 Rangoon 280: GMT 07:00 Bangkok, Hanoi, Jakarta,

			Krasnoyarsk 320: GMT 08:00 Beijing, Chongging, Hong Kong, Kuala Lumpur, Singapore, Taipei 360: GMT 09:00 Osaka, Sapporo, Tokyo, Seoul, Yakutsk 380: GMT 09:30 Adelaide, Darwin 400: GMT 10:00 Brisbane, Canberra, Melbourne, Sydney, Guam, Vladivostok 440: GMT 11:00 Magadan, Solomon Is., New Caledonia 480: GMT 12:00 Aucklan, Wellington, Fiji, Kamchatka, Marshall Is. 520: GMT 13:00 Nuku'Alofa
daylight_enable	<boolean>	6/6	Enable automatic daylight saving time in time zone.
daylight_dstactualmode	<boolean>	6/7	Check if current time is under daylight saving time.
daylight_auto_begintime	string[19]	6/7	Display the current daylight saving start time. (product dependent)
daylight_auto_endtime	string[19]	6/7	Display the current daylight saving end time. (product dependent)
updateinterval	0, 3600, 86400, 604800, 2592000	6/6	0 to Disable automatic time adjustment, otherwise, it indicates the seconds between NTP automatic update intervals.

Subgroup of **system**: **info** (The fields in this group are unchangeable.)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
modelname	string[40]	0/7	Internal model name of the server (eg. IP7139)
serialnumber	<mac address>	0/7	12 characters MAC address (without hyphens).
firmwareversion	string[40]	0/7	Firmware version, including model, company, and version number in the format: <MODEL-BRAND-VERSION>
language_i<0~(count-1)>	string[16]	0/7	Available language lists.

Group: **status**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
di_i<0~(ndi-1)>	<boolean>	1/7	0 => Inactive, normal 1 => Active, triggered
do_i<0~(ndo-1)>	<boolean>	1/7	0 => Inactive, normal 1 => Active, triggered
onlinenum_rtsp	integer	6/7	Current number of RTSP connections.
onlinenum_httppush	integer	6/7	Current number of HTTP push server connections.

Group: **di_i<0~(ndi-1)>** (capability.ndi > 0)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
normalstate	high, low	1/1	Indicates open circuit or closed circuit (inactive status)

Group: **do_i<0~(ndo-1)>** (capability.ndo > 0)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
normalstate	open, grounded	1/1	Indicate open circuit or closed circuit (inactive status)

Group: **security**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
user_i0_name	string[64]	6/7	User name of root
user_i<1~20>_name	string[64]	6/7	User name
user_i0_pass	password[64]	6/6	Root password
user_i<1~20>_pass	password[64]	7/6	User password
user_i0_privilege	viewer, operator, admin	6/7	Root privilege
user_i<1~20>_ privilege	viewer, operator, admin	6/6	User privilege

Group: **network**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
type	lan, pppoe	6/6	Network connection type.
preprocess	0~15	6/6	Stop related process before setting port value.
resetip	<boolean>	6/6	1 => Get ipaddress, subnet, router, dns1, dns2 from DHCP server at next reboot. 0 => Use preset ipaddress, subnet, rounter, dns1, and dns2.
ipaddress	<ip address>	6/6	IP address of server.
subnet	<ip address>	6/6	Subnet mask.
router	<ip address>	6/6	Default gateway.
dns1	<ip address>	6/6	Primary DNS server.
dns2	<ip address>	6/6	Secondary DNS server.
wins1	<ip address>	6/6	Primary WINS server.
wins2	<ip address>	6/6	Secondary WINS server.

Subgroup of **network**: **ftp**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	21, 1025~65535	6/6	Local ftp server port.

Subgroup of **network**: **http**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	80, 1025 ~ 65535	6/6	HTTP port.
alternateport	1025~65535	6/6	Alternate HTTP port.
authmode	basic, digest	1/6	HTTP authentication mode.
s0_accessname	string[32]	1/6	HTTP server push access name for stream 1. (capability.protocol.spush_mjpeg =1 and video.stream.count>0)
s1_accessname	string[32]	1/6	HTTP server push access name for stream 2. (capability.protocol.spush_mjpeg =1 and video.stream.count>1)

Subgroup of **network**: **rtsp**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	554, 1025 ~ 65535	1/6	RTSP port. (capability.protocol.rtsp=1)
authmode	disable, basic, digest	1/6	RTSP authentication mode. (capability.protocol.rtsp=1)
s0_accessname	string[3b;42]	1/6	RTSP access name for stream1. (capability.protocol.rtsp=1 and video.stream.count>0)
s1_accessname	string[32]	1/6	RTSP access name for stream2. (capability.protocol.rtsp=1 and video.stream.count>1)
s0_audiotrack	<integer>	6/6	The current audio track for stream1. -1 => audio mute
s1_audiotrack	<integer>	6/6	The current audio track for stream2. -1 => audio mute

Subgroup of **network_rtsp_s<0~(n-1)>**: **multicast,** n is stream count

(capability.protocol.rtp.multicast=1)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
alwaysmulticast	<boolean>	4/4	Enable always multicast.
ipaddress	<ip address>	4/4	Multicast IP address.
videoport	1025 ~ 65535	4/4	Multicast video port.
audioport	1025 ~ 65535	4/4	Multicast audio port.
ttl	1 ~ 255	4/4	Mutlicast time to live value.

Subgroup of **network**: **rtp**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
videoport	1025 ~ 65535	6/6	Video channel port for RTP. (capability.protocol.rtp_unicast=1)
audioport	1025 ~ 65535	6/6	Audio channel port for RTP. (capability.protocol.rtp_unicast=1)

Subgroup of **network**: **pppoe**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
user	string[128]	6/6	PPPoE account user name.
pass	password[64]	6/6	PPPoE account password.

Group: **wireless**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
ssid	string[32]	6/6	SSID for wireless lan settings. The valid characters are [A-Z] [a-z] [0-9] [/] [.] [_] [=] [ ] [-] [+] [*].
wlmode	Infra, Adhoc	6/6	Wireless mode. Infra: Infrastructure
channel	1~11 or 1 ~ 13 or 10~11 or 10~13 or 1~14	6/6	USA and Canada Europe Spain France All
txrate	NONE, 1M, 2M, 5.5M, 11M, 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M, Auto	6/6	Maximum boolean rate in Mbps.
encrypt	0~3	6/6	Encryption method (product dependent): 0=> NONE, 1 => WEP, 2 => WPA, 3 => WPA2PSK
authmode	OPEN, SHARED	6/6	Authentication mode.
keylength	64, 128	6/6	Key length in bits.
keyformat	HEX, ASCII	6/6	Key1 ~ key4 presentation format.
keyselect	1 ~ 4	6/6	Default key number.
key1	password [32]	6/6	WEP key1 for encryption. The valid characters are [A-Z] [a-z] [0-9].
key2	password [32]	6/6	WEP key2 for encryption. The valid characters are [A-Z] [a-z] [0-9].
key3	password [32]	6/6	WEP key3 for encryption. The valid characters are [A-Z] [a-z] [0-9].

key4	password [32]	6/6	WEP key4 for encryption. The valid characters are [A-Z] [a-z] [0-9].
domain	'U' for USA 'C' for Canada 'E' for Euro 'S' for Spain 'F' for France 'I' for Isrel 'A' for All	6/7	Wireless domain.
algorithm	AES, TKIP	6/6	Algorithm
presharedkey	password [63]	6/6	WPA mode pre-shared key. The valid characters are [A-Z] [a-z] [0-9].

Group: **ipfilter**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
allow_i<0~9>_start	1.0.0.0 ~ 255.255.255.255	6/6	Allowed starting IPv4 address for connection.
allow_i<0~9>_end	1.0.0.0 ~ 255.255.255.255	6/6	Allowed ending IPv4 address for connection.
deny_i<0~9>_start	1.0.0.0 ~ 255.255.255.255	6/6	Denied starting IPv4 address for connection.
deny_i<0~9>_end	1.0.0.0 ~ 255.255.255.255	6/6	Denied ending IPv4 address for connection.

Group: **videoin**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
cmosfreq	50, 60	4/4	CMOS frequency. (videoin.type=2) (product dependent)
whitebalance	<product dependent>	4/4	Auto, auto white balance: Manual Indoor, 3200K Fluorescent, 5500K Outdoor, > 5500K
atwbvalue	<product dependent>	4/4	Auto white balance value
privacystatus	<boolean>	4/4	Video privacy status When privacy button is "on", video will become blue-screen.

Group: **videoin_c<0~(n-1)>** for n channel products, and m is stream number

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
color	0, 1	4/4	0 =>monochrome 1 => color
flip	<boolean>	4/4	Flip the image.
mirror	<boolean>	4/4	Mirror the image.
ptzstatus	<integer>	1/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support camera control function; 0(not support), 1(support) Bit 1 => **Built-in** or **external** camera; 0 (external), 1(built-in) Bit 2 => Support **pan** operation; 0(not support), 1(support) Bit 3 => Support **tilt** operation; 0(not support), 1(support) Bit 4 => Support **zoom** operation; 0(not support), 1(support) Bit 5 => Support **focus** operation; 0(not support), 1(support)
text	string[16]	1/4	Enclose caption.
imprinttimestamp	<boolean>	4/4	Overlay time stamp on video.
maxexposure	1~120	4/4	Maximum exposure time.
options	quality, framerate	4/4	Customize video quality first or video frame rate first. (product dependent)
s<0~(m-1)>_codectype	mpeg4, mjpeg	1/4	Video codec type.
s<0~(m-1)>_resolution	VGA CMOS => 176x144, 160x120, 320x240, 640x480 3M CMOS => 176x144, 320x240, 640x480, 800x600, 1280x1024	1/4	Video resolution in pixels.

	CCD => QCIF, 176x120, CIF, 352x240, 4CIF, 704x480 PAL => QCIF, 176x144, CIF, 352x288, 4CIF, 704x576 VS => QCIF, 176x120, 176x144, CIF, 352x240, 352x288, 4CIF, 704x480, 704x576		
s<0~(m-1)>_mpeg4_intraperiod	250, 500, 1000, 2000, 3000, 4000	4/4	Intra frame period in milliseconds.
s<0~(m-1)>_mpeg4_ratecontrolmode	cbr, vbr	4/4	cbr, constant bitrate vbr, fix quality
s<0~(m-1)>_mpeg4_quant	0, 1~5	4/4	Quality of video when choosing vbr in “ratecontrolmode”. 0 is the customized manual input setting. 1 = worst quality, 5 = best quality.
s<0~(m-1)>_mpeg4_bitrate	1000~8000000	4/4	Set bit rate in bps when choosing cbr in “ratecontrolmode”.
s<0~(m-1)>_mpeg4_maxframe	1~25, 26~30 (only for NTSC or 60Hz	1/4	Set maximum frame rate in fps (for MPEG-4).

	CMOS)		
s<0~(m-1)>_mjpeg_quant	0 ~ 5	4/4	Quality of JPEG video. 0 is the customized manual input setting. 1 = worst quality, 5 = best quality.
s<0~(m-1)>_mjpeg_maxframe	1~25, 26~30 (only for NTSC or 60Hz CMOS)	1/4	Set maximum frame rate in fps (for JPEG).

Group: **audioin_c<0~(n-1)>** for n channel products (capability.audioin>0)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
source	micin, linein	4/4	Micin => use external microphone input. Linein => use line input.
mute	0, 1	4/4	Enable audio mute.
gain	0~31	4/4	Gain of input.
s<0~(m-1)>_codectype	aac4, gamr	4/4	Set audio codec type for input.
s<0~(m-1)>_aac4_bitrate	16000, 32000, 48000, 64000, 96000, 128000	4/4	Set AAC4 bitrate in bps.
s<0~(m-1)>_gamr_bitrate	4750, 5150, 5900, 6700, 7400, 7950, 10200, 12200	4/4	Set AMR bitrate in bps.

Group: **image_c<0~(n-1)>** for n channel products

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
brightness	<product dependent>	4/4	Adjust brightness of image according to mode settings.
saturation	-5 ~ 5	4/4	Adjust saturation of image according to mode settings.
contrast	-5 ~ 5	4/4	Adjust contrast of image according to mode settings.
sharpness	<product dependent>	4/4	Adjust sharpness of image according to mode settings.

Group: **imagepreview_c<0~(n-1)>** for n channel products

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
brightness	<product dependent>	4/4	Preview of brightness adjustment of image according to mode settings.
saturation	-5 ~ 5	4/4	Preview of saturation adjustment of image according to mode settings.
contrast	-5 ~ 5	4/4	Preview of contrast adjustment of image according to mode settings.
sharpness	<product dependent>	4/4	Preview of sharpness adjustment of image according to mode settings.
videoin_whitebalance	auto, manual	4/4	Preview of white balance adjustment of image according to mode settings.
videoin_restoreatwb	0, 1~	4/4	Restore white balance adjustment of image according to mode settings.

Group: **imagepreview**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
videoin_whitebalance	auto, manual	4/4	Preview of adjusting white balance of image according to mode settings
videoin_restoreatwb	0, 1~	4/4	Restore of adjusting white balance of image according to mode settings

Group: **motion_c<0~(n-1)>** for m profile and n channel product

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	4/4	Enable motion detection.
win_i<0~2>_enable	<boolean>	4/4	Enable motion window 1~3.
win_i<0~2>_name	string[14]	4/4	Name of motion window 1~3.
win_i<0~2>_left	0 ~ 320	4/4	Left coordinate of window position.
win_i<0~2>_top	0 ~ 240	4/4	Top coordinate of window position.
win_i<0~2>_width	0 ~ 320	4/4	Width of motion detection window.
win_i<0~2>_height	0 ~ 240	4/4	Height of motion detection window.
win_i<0~2>_objsize	0 ~ 100	4/4	Percent of motion detection window.
win_i<0~2>_sensitivity	0 ~ 100	4/4	Sensitivity of motion detection window.

Group: **ddns**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable or disable the dynamic DNS.

provider	Safe100,
	DyndnsDynamic,
	DyndnsCustom,
	TZO,
	DHS,
	DynInterfree,
	CustomSafe100
		6/6	Safe100 => safe100.net
			DyndnsDynamic => dyndns.org (dynamic)
			DyndnsCustom => dyndns.org (custom)
			TZO => tzo.com
			DHS => dhs.org
			DynInterfree =>dyn-interfree.it
			CustomSafe100 =>
			Custom server using safe100 method

<provider>_hostname	string[128]	6/6	Your dynamic hostname.
<provider>_usernameemail	string[64]	6/6	Your user or email to login to the DDNS service provider
<provider>_passwordkey	string[64]	6/6	Your password or key to login to the DDNS service provider.
<provider>_servername	string[128]	6/6	The server name for safe100. (This field only exists if the provider is customsafe100)
update	<boolean>	6/7	Update ddns

Group: **upnppresentation**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable or disable the UPNP presentation service.

Group: **upnpportforwarding**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable or disable the UPNP port forwarding service.
upnpnatstatus	0~3	6/7	The status of UpnP port forwarding, used internally. 0 = OK, 1 = FAIL, 2 = no IGD router, 3 = no need for port forwarding

Group: **syslog**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enableremotelog	<boolean>	6/6	Enable remote log.

serverip	<IP address>	6/6	Log server IP address.
serverport	514, 1025~65535	6/6	Server port used for log.
level	0~7	6/6	Levels used to distinguish the importance of the information: 0: LOG_EMERG 1: LOG_ALERT 2: LOG_CRIT 3: LOG_ERR 4: LOG_WARNING 5: LOG_NOTICE 6: LOG_INFO 7: LOG_DEBUG

Group: **privacymask_c<0~(n-1)>** for n channel product

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	4/4	Enable privacy mask.
win_i<0~4>_enable	<boolean>	4/4	Enable privacy mask window.
win_i<0~4>_name	string[14]	4/4	Name of the privacy mask window.
win_i<0~4>_left	0 ~ 320/352	4/4	Left coordinate of window position.
win_i<0~4>_top	0 ~ 240/288	4/4	Top coordinate of window position.
win_i<0~4>_width	0 ~ 320/352	4/4	Width of privacy mask window.
win_i<0~4>_height	0 ~ 240/288	4/4	Height of privacy mask window.
win_i<0~4>_color	0 ~ 13	4/4	Color of privacy mask window.

Group: capability

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
api_httpversion	0100a	0/7	The HTTP API version.
bootuptime	<positive integer>	0/7	Server bootup time.
nir	0, <positive integer>	0/7	Number of IR interfaces.
ndi	0, <positive integer>	0/7	Number of digital inputs.
ndo	0, <positive integer>	0/7	Number of digital outputs.
naudioin	0, <positive integer>	0/7	Number of audio inputs.

naudioout	0, <positive integer>	0/7	Number of audio outputs.
nvideoin	<positive integer>	0/7	Number of video inputs.
nmediastream	<positive integer>	0/7	Number of media stream per channels.
nvideosetting	<positive integer>	0/7	Number of video settings per channel.
naudiosetting	<positive integer>	0/7	Number of audio settings per channel.
nuart	0, <positive integer>	0/7	Number of UART interfaces.
ptzenabled	<positive integer>	0/7	An 32-bit integer, each bit can be set separately as follows: Bit 0 => Support camera control function; 0(not support), 1(support) Bit 1 => Built-in or external camera; 0(external), 1(built-in) Bit 2 => Support pan operation, 0(not support), 1(support) Bit 3 => Support tilt operation; 0(not support), 1(support) Bit 4 => Support zoom operation; 0(not support), 1(support) Bit 5 => Support focus operation; 0(not support), 1(support) Bit 6 => Support iris operation; 0(not support), 1(support) Bit 7 => External or built-in PT; 0(built-in), 1(external) Bit 8 => Invalidate bit 1 ~ 7; 0(bit 1 ~ 7 are valid), 1(bit 1 ~ 7 are invalid) Bit 9 => Reserved bit; Invalidate lens_pan, Lens_tilt, lens_zoon, lens_focus, len_iris. 0(fields are valid), 1(fields are invalid)
protocol_https	< boolean >	0/7	Indicate whether to support HTTP over SSL.
protocol_rtsp	< boolean >	0/7	Indicate whether to support RTSP.
protocol_sip	<boolean>	0/7	Indicate whether to support SIP.
protocol_maxconnection	<positive integer>	0/7	The maximum allowed simultaneous connections.
protocol_rtp_multic	<boolean>	0/7	Indicate whether to support scalable

ast_scalable			multicast.
protocol_rtp_multicast_backchannel	<boolean>	0/7	Indicate whether to support backchannel multicast.
protocol_rtp_tcp	<boolean>	0/7	Indicate whether to support RTP over TCP.
protocol_rtp_http	<boolean>	0/7	Indicate whether to support RTP over HTTP.
protocol_spush_mjpeg	<boolean>	0/7	Indicate whether to support server push MJPEG.
protocol_snmp	<boolean>	0/7	Indicate whether to support SNMP.
videoin_type	0, 1, 2	0/7	0 => Interlaced CCD 1 => Progressive CCD 2 => CMOS
videoin_resolution	<a list of available resolution separated by commas>	0/7	Available resolutions list.
videoin_codec	<a list of available codec types separated by commas>	0/7	Available codec list.
videoout_codec	<a list of the available codec types separated by commas)	0/7	Available codec list.
audio_aec	<boolean>	0/7	Indicate whether to support acoustic echo cancellation.
audio_extmic	<boolean>	0/7	Indicate whether to support external microphone input.
audio_linein	<boolean>	0/7	Indicate whether to support external line input.
audio_lineout	<boolean>	0/7	Indicate whether to support line output.
audio_headphoneout	<boolean>	0/7	Indicate whether to support headphone output.
audioin_codec	<a list of the available codec types separated by commas)	0/7	Available codec list.
audioout_codec	<a list of the available codec types separated by commas)	0/7	Available codec list.

uart_httptunnel	<boolean>	0/7	Indicate whether to support HTTP tunnel for UART transfer.
transmission_mode	Tx, Rx, Both	0/7	Indicate transmission mode of the machine: TX = server, Rx = receiver box, Both = DVR.
network_wire	<boolean>	0/7	Indicate whether to support Ethernet.
network_wireless	<boolean>	0/7	Indicate whether to support wireless.
wireless_s802dot11b	<boolean>	0/7	Indicate whether to support wireless 802.11b+.
wireless_s802dot11g	<boolean>	0/7	Indicate whether to support wireless 802.11g.
wireless_beginchannel	1 ~ 14	0/7	Indicate the begin channel of wireless network
wireless_endchannel	1 ~ 14	0/7	Indicate the end channel of wireless network
wireless_encrypt_wep	<boolean>	0/7	Indicate whether to support wireless WEP.
wireless_encrypt_wpa	<boolean>	0/7	Indicate whether to support wireless WPA.
wireless_encrypt_wpa2	<boolean>	0/7	Indicate whether to support wireless WPA2.
derivative_brand	<boolean>	0/7	Indicate whether to support the upgrade function for the derivative brand. For example, if the value is true, the VVTK product can be upgraded to VVXX. (TCVV<->TCXX is excepted)

Group: **event_i**<0~2>

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	Identification of this entry.
enable	0, 1	6/6	Enable or disable this event.
priority	0, 1, 2	6/6	Indicate the priority of this event: “0” = low priority “1” = normal priority “2” = high priority
delay	1~999	6/6	Delay in seconds before detecting the next event.

trigger	boot, di, motion, seq, visignal, pir, recnotify, audioswitch, tampering, iva	6/6	Indicate the trigger condition: “boot” = System boot “di”= Digital input “motion” = Video motion detection “seq” = Periodic condition “visignal” = Video input signal loss. “pir” = PIR detection. “recnotify” = Recording notification. “audioswitch” = Audio switch. “tampering” = Tamper detection. “iva” = IVA trigger.
di	<integer>	6/6	Indicate which DI detects. This field is required when trigger condition is “di”. One bit represents one digital input. The LSB indicates DI 0.
mdwin	<integer>	6/6	Indicate which motion detection windows detect. This field is required when trigger condition is “md”. One bit represents one window. The LSB indicates the 1st window. For example, to detect the 1st and 3rd windows, set mdwin as 5.
mdwin0	<integer>	6/6	Indicate which motion detection windows of profile 1 detect.
inter	1~999	6/6	Interval of snapshots in minutes. This field is used when trigger condition is “seq”.

weekday	<integer>	6/6	Indicate which weekday is scheduled.
			One bit represents one weekday.
			bit0 (LSB) = Saturday
			bit1 = Friday
			bit2 = Thursday
			bit3 = Wednesday
			bit4 = Tuesday
			bit5 = Monday
			bit6 = Sunday
			For example, to detect events on Friday and Sunday, set weekday as 66.

begintime	hh:mm	6/6	Begin time of the weekly schedule.
endtime	hh:mm	6/6	End time of the weekly schedule. (00:00 ~ 24:00 sets schedule as always on)

action_do_i<0~(ndo-1)>_enable	0, 1	6/6	Enable or disable trigger digital output.
action_do_i<0~(ndo-1)>_duration	1~999	6/6	Duration of the digital output trigger in seconds.
action_server_i<0~4>_enable	0, 1	6/6	Enable or disable this server action. The default value is 0.
action_server_i<0~4>_media	NULL, 0~4	6/6	Index of the attached media.

Group: **server_i**<0~4>

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	Identification of this entry
type	email, ftp, http, ns	6/6	Indicate the server type: “email” = email server “ftp” = FTP server “http” = HTTP server “ns” = network storage
http_url	string[128]	6/6	URL of the HTTP server to upload.
http_username	string[64]	6/6	Username to log in to the server.
http_passwd	string[64]	6/6	Password of the user.
ftp_address	string[128]	6/6	FTP server address.
ftp_username	string[64]	6/6	Username to log in to the server.
ftp_passwd	string[64]	6/6	Password of the user.
ftp_port	0~65535	6/6	Port to connect to the server.
ftp_passive	0, 1	6/6	Enable or disable passive mode. 0 = disable passive mode 1 = enable passive mode
email_address	string[128]	6/6	Email server address.
email_username	string[64]	6/6	Username to log in to the server.
email_passwd	string[64]	6/6	Password of the user.
email_senderemail	string[128]	6/6	Email address of the sender.
email_recipientemail	string[128]	6/6	Email address of the recipient.

Group: **media_i<0~4>** (media_freespace is used internally.)

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	Identification of this entry

type	snapshot, systemlog, videoclip, recordmsg	6/6	Media type to send to the server or store on the server.
snapshot_source	<integer>	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc. 2 means the third stream and etc. 3 means the fourth stream and etc.
snapshot_prefix	string[16]	6/6	Indicate the prefix of the filename.
snapshot_datesuffix	0, 1	6/6	Add date and time suffix to filename: 1 = Add date and time suffix. 0 = Do not add.
snapshot_preevent	0 ~ 7	6/6	Indicates the number of pre-event images.
snapshot_postevent	0 ~ 7	6/6	The number of post-event images.
videoclip_source	<integer>	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc. 2 means the third stream and etc. 3 means the fourth stream and etc.
videoclip_prefix	string[16]	6/6	Indicate the prefix of the filename.
videoclip_preevent	0 ~ 9	6/6	Indicates the time for pre-event recording in seconds.
videoclip_maxduration	1 ~ 10	6/6	Maximum duration of one video clip in seconds.
videoclip_maxsize	50 ~ 600	6/6	Maximum size of one video clip file in Kbytes.

Drive the Digital Output

Note: This request requires Viewer privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/dido/setdo.cgi?do1=<*state*>[&do2=<state>]
[&do3=<state>][&do4=<state>][&return=<*return page*>]

Where state is 0 or 1; "0" means inactive or normal state, while "1" means active or triggered state.

PARAMETER	VALUE	DESCRIPTION
do<num>	0, 1	0 – Inactive, normal state
		1 – Active, triggered state
return	*<return page>*	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

Example: Drive the digital output 1 to triggered state and redirect to an empty page.

```
http://myserver/cgi-bin/dido/setdo.cgi?do1=1
```

Query Status of the Digital Input

Note: This request requires Viewer privileges.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/dido/getdi.cgi?[di0][&di1][&di2][&di3]
```

If no parameter is specified, all of the digital input statuses will be returned.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <length>\r\n
\r\n
[di0=<state>]\r\n
[di1=<state>]\r\n
[di2=<state>]\r\n
[di3=<state>]\r\n
```

where *<state>* can be 0 or 1.

Example: Query the status of digital input 1.

```
Request:
http://myserver/cgi-bin/dido/getdi.cgi?di1

Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: 7\r\n
\r\n
di1=1\r\n
```

Query Status of the Digital Output

Note: This request requires Viewer privileges.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/dido/getdo.cgi?[do0][&do1][&do2][&do3]
```

If no parameter is specified, all the digital output statuses will be returned.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <length>\r\n
\r\n
[do0=<state>]\r\n
[do1=<state>]\r\n
[do2=<state>]\r\n
[do3=<state>]\r\n
```

where *<state>* can be 0 or 1.

Example: Query the status of digital output 1.

```
Request:
http://myserver/cgi-bin/dido/getdo.cgi?do1

Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
```

```
Content-Length: 7\r\n
\r\n
do1=1\r\n
```

Capture Single Snapshot

Note: This request requires Normal User privileges.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/viewer/video.jpg?[channel=<value>][&resolution=<value>]
[&quality=<value>]
```

If the user requests a size larger than all stream settings on the server, this request will fail.

PARAMETER	VALUE	DEFAULT	DESCRIPTION
channel	0~(n-1)	0	The channel number of the video source.
resolution	*<available resolution>*	0	The resolution of the image.
quality	*1~5*	3	The quality of the image.

The server will return the most up-to-date snapshot of the selected channel and stream in JPEG format. The size and quality of the image will be set according to the video settings on the server.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: image/jpeg\r\n
[Content-Length: <image size>\r\n]

<binary JPEG image data>
```

Account Management

Note: This request requires Administrator privileges.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/admin/editaccount.cgi?
```

```
method=<value>&username=<name>[&userpass=<value>][&privilege=<value>]
[&privilege=<value>][…][&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
method	Add	Add an account to the server. When using this method, the "username" field is necessary. It will use the default value of other fields if not specified.
	Delete	Remove an account from the server. When using this method, the "username" field is necessary, and others are ignored.
	edit	Modify the account password and privilege. When using this method, the "username" field is necessary, and other fields are optional. If not specified, it will keep the original settings.
username	<name>	The name of the user to add, delete, or edit.
userpass	<value>	The password of the new user to add or that of the old user to modify. The default value is an empty string.
privilege	<value>	The privilege of the user to add or to modify.
	viewer	Viewer privilege.
	operator	Operator privilege.
	admin	Administrator privilege.
return	<return page>	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

System Logs

Note: This request require Administrator privileges.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/admin/syslog.cgi
```

Server will return the most up-to-date system log.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <syslog length>\r\n
\r\n
<system log information>\r\n
```

Upgrade Firmware

Note: This request requires Administrator privileges.

Method: POST

Syntax:

```
http://<servername>/cgi-bin/admin/upgrade.cgi
```

Post data:

```
fimage=<file name>[&return=<return page>]\r\n
\r\n
<multipart encoded form data>
```

Server will accept the file named <file name> to upgrade the firmware and return with <return page> if indicated.

System Information

Note: This request requires Normal User privileges. (obsolete)

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/sysinfo.cgi
```

Server will return the system information. In HTTP API version 2, the CapVersion will be 0200. All fields in the previous version (0100) are obsolete. Please use “getparam.cgi?capability” instead.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <system information length>\r\n
\r\n
Model=<model name of server>\r\n
CapVersion=0200\r\n
```

PARAMETER(supported capability version)	VALUE	DESCRIPTION
Model	system.firmwareversion	Model name of the server. Ex:IP3133-VVTK-0100a
CapVersion	*MMmm, MM is major version from 00 ~ 99* *mm is minor version from 00 ~ 99* *ex: 0100*	Capability field version.

IP Filtering

Note: This request requires Administrator access privileges.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/admin/ipfilter.cgi?
method=<value>&[start=<ipaddress>&end=<ipaddress>][&index=<value>]
[&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
Method	addallow	Add allowed IP address range to the server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from the index position.
	adddeny	Add denied IP address range to the server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from the index position.
	deleteallow	Remove allowed IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter.
	deletedeny	Remove denied IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter.
start	<ip address>	The starting IP address to add or to delete.
end	<ip address>	The ending IP address to add or to delete.
index	<value>	The start position to add or to delete.

return	<return page>	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

Get SDP of Streams

Note: This request requires Viewer access privileges.

Method: GET/POST

Syntax:

```
http://<servername>/<network_rtsp_s<0~m-1>_accessname>
```

“m” is the stream number.

“network_accessname_<0~(m-1)>” is the accessname for stream “1” to stream “m”. Please refer to the “subgroup of network: rtsp” for setting the accessname of SDP.

You can get the SDP by HTTP GET.

Open the Network Stream

Note: This request requires Viewer access privileges.

Syntax:

For HTTP push server (MJPEG):

```
http://<servername>/<network_http_s<0~m-1>_accessname>
```

For RTSP (MP4), the user needs to input the URL below into an RTSP compatible player.

```
rtsp://<servername>/<network_rtsp_s<0~m-1>_accessname>
```

“m” is the stream number.

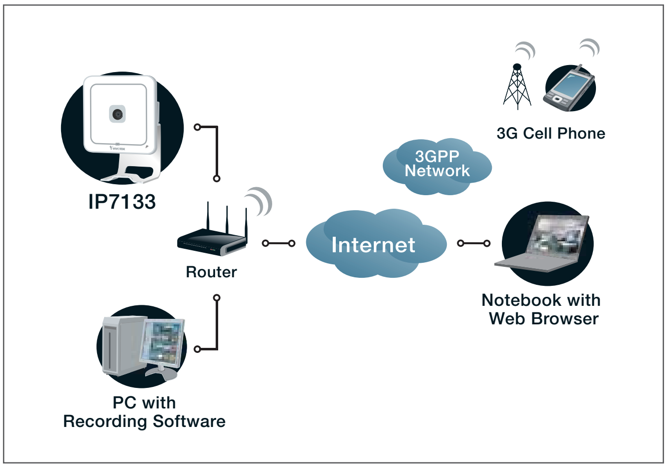
For details on streaming protocol, please refer to the “control signaling” and “data format” documents.

Technical Specifications

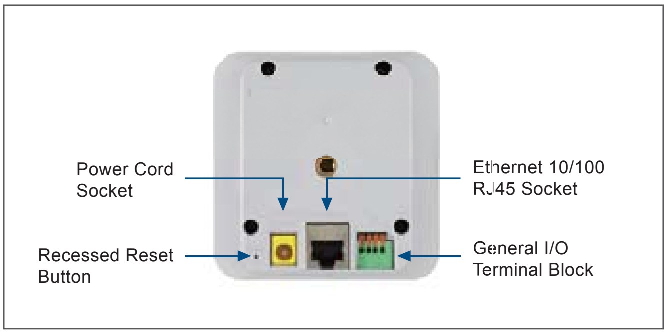
Models	· IP7133 (Wired) · IP7134 (WLAN)
System	· CPU: VVTK-1000 SoC · Flash: 4MB · RAM: 32MB · Embedded OS: Linux 2.4
Lens	· Board lens, f = 4.09 mm, F2.0, Fixed, focus range: 70 cm to infinity
Angle of View	· 49.6° (horizontal) · 38.2° (vertical)
Shutter Time	· 1/5 sec. to 1/15,000 sec.
Image Sensor	· 1/4" CMOS sensor in VGA resolution
Minimum Illumination	· 0.4 Lux / F2.0
Video	· Compression: MJPEG & MPEG-4 · Streaming: Simultaneous dual-streaming MPEG-4 streaming over UDP, TCP or HTTP MPEG-4 multicast streaming MJPEG streaming over HTTP · Supports 3GPP mobile surveillance · Frame rates: MPEG-4: Up to 30/25 fps at 640x480 MJPEG: Up to 30/25 fps at 640x480
Image Settings	· Adjustable image size, quality and bit rate · Time stamp and text caption overlay · Flip & mirror · Configurable brightness, contrast, saturation, sharpness and white balance · AGC, AWB, AES · Supports privacy masks
Audio	· Compression: GSM-AMR speech encoding,bit rate: 4.75 kbps to 12.2 kbps MPEG-4 AAC audio encoding,bit rate: 16 kbps to 128 kbps · Interface: Built-in microphone · Supports audio mute
Networking	· 10/100 Mbps Ethernet, RJ-45 · Built-in 802.11b/g WLAN (IP7134) · Protocols: IPv4, TCP/IP, HTTP, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS and PPPoE
Alarm and Event Management	· Triple-window video for motion detection · One D/I and one D/O for external sensor and alarm · Event notification using HTTP, SMTP or FTP · Local recording of MP4 file
Security	· Muilti-level user access with password protection · IP address filtering · Wireless: WEP, WPA-PSK, WPA2 (IP7134)
Users	· Live viewing for up to 10 clients
Dimension	· 26.9 mm (D) x 86.7 mm (W) x 87.6 mm (H)
Weight	· Net: 106 g (IP7133) · Net: 122 g (IP7134)

LED Indicator	· System power and status indicator · System activity and network link indicator · Privacy button on
Power	· 5V DC · Power consumption: Max. 5 W (IP7133) Max. 6.6 W (IP7134)
Approvals	· CE, LVD, FCC, VCCI
Operating Environments	· Temperature: 0 ~ 40 °C (32 ~ 102 °F) · Humidity: 20% ~ 80% RH
Viewing System Requirements	· OS: Microsoft Windows 2000/XP/Vista · Browser: Mozilla Firefox, Internet Explorer 6.x or above · Cellp phone: 3GPP player · Real Player: 10.5 or above · Quick Time: 6.5 or above
Installation, Management, and Maintenance	· Installation Wizard 2 · 16-CH recording software · Supports firmware upgrade
Applications	· SDK available for application development and system integration
Warranty	· 12 months

System overview



External View



Technology License Notice

MPEG-4 AAC Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 AAC AUDIO PATENT LICENSE. THIS PRODUCT MAY NOT BE DECOMPILED, REVERSE-ENGINEERED OR COPIED, EXCEPT REGARD TO PC SOFTWARE, YOU MAY MAKE SINGLE COPIES FOR ARCHIVAL PURPOSES. FOR MORE INFORMATION, PLEASE REFER TO HTTP://WWW.VIALICENSING.COM.

MPEG-4 Visual Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 VISUAL PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER FOR (i) ENCODING VIDEO IN COMPLIANCE WITH THE MPEG-4 VISUAL STANDARD ("MPEG-4 VIDEO") AND/OR (ii) DECODING MPEG-4 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED BY MPEG LA TO PROVIDE MPEG-4 VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION INCLUDING THAT RELATING TO PROMOTIONAL, INTERNAL AND COMMERCIAL USES AND LICENSING MAY BE OBTAINED FROM MPEG LA, LLC. PLEASE REFER TO HTTP://WWW.MPEGLA.COM.

AMR-NB Standard

THIS PRODUCT IS LICENSED UNDER THE AMR-NB STANDARD PATENT LICENSE AGREEMENT. WITH RESPECT TO THE USE OF THIS PRODUCT, THE FOLLOWING LICENSORS' PATENTS MAY APPLY:

TELEFONAKIEBOLAGET ERICSSON AB: US PAT. 6192335; 6275798; 6029125; 6424938; 6058359. NOKIA CORPORATION: US PAT. 5946651; 6199035. VOICEAGE CORPORATION: AT PAT. 0516621; BE PAT. 0516621; CA PAT. 2010830; CH PAT. 0516621; DE PAT. 0516621; DK PAT. 0516621; ES PAT. 0516621; FR PAT. 0516621; GB PAT. 0516621; GR PAT. 0516621; IT PAT. 0516621; LI PAT. 0516621; LU PAT. 0516621; NL PAT. 0516621; SE PAT 0516621; US PAT 5444816; AT PAT. 819303/AT E 198805T1; AU PAT. 697256; BE PAT. 819303; BR PAT. 9604838-7; CA PAT. 2216315; CH PAT. 819303; CN PAT. ZL96193827.7; DE PAT. 819303/DE69611607T2; DK PAT. 819303; ES PAT. 819303; EP PAT. 819303; FR PAT. 819303; GB PAT. 819303; IT PAT. 819303; JP PAT. APP. 8-529817; NL PAT. 819303; SE PAT. 819303; US PAT. 5664053. THE LIST MAY BE UPDATED FROM TIME TO TIME BY LICENSORS AND A CURRENT VERSION OF WHICH IS AVAILABLE ON LICENSOR'S WEBSITE AT HTTP://WWW.VOICEAGE.COM.

Electromagnetic Compatibility (EMC)

FCC Statement

This device compiles with FCC Rules Part 15. Operation is subject to the following two conditions.

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a partial installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Shielded interface cables must be used in order to comply with emission limits.

CE Mark Warning CE (!)

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

This device (IP7134) complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC.

This device (IP7134) is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device (IP7134) may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

Liability

VIVOTEK Inc. cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. VIVOTEK Inc. makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for any particular purpose.